

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة منتوري – قسنطينة



كلية العلوم الإنسانية والعلوم الاجتماعية

قسم علم المكتبات

الرقم التسلسلي:.........................

التهديدات الأمنية للمواقع الالكترونية للجامعة الجزائرية

دراسة حالة الموقع الالكتروني لجامعة منتوري –قسنطينة-

مذكرة مقدمة لنيل شهادة المـاستــر في علم المكتبات

تخصص: تكنولوجيا جديدة وأنظمة المعلومات

إعداد الطالبين :

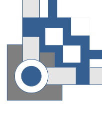
- ذياب كريم
- روان محمد.

لجنة المناقشة :

د. طاشور محمد.. مشرفًا ومقرّرًا

أ. سعيدي سليمة .... منـاقشـًا

جوان 2011




بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله نستعينه ونحمده ونشكره على فضله علينا، والذي لو لا عونه لنا وتوفيقه لما استطعنا إنجاز هذا العل المتواضع. والذي نرجو أن يكلل بالنجاح.

أتقدم بالشكر الجزيل للدكتور " طاشور محمد " لإشرافه على إنجاز هذا العل وتعاونه الصادق، وسعة صدره، وصبره علينا، وعلى كل توجيهاته لنا التي كان لها الأثر البالغ فيما وصلنا إليه.

أسأل الله الكريم أن يجعل ذلك في ميزان حسناته.

إلى كل من ساهم في المساعدة لإتمام هذا العل المتواضع، بنصيحة أو بكلمة طيبة.

أدعوا الله أن يجازيهم الجزاء الأوفى. إنه ولي ذلك والقادر عليه.



الإهداء

إلى الذي كان دوما إلى جانبي ...صاحب الفضل ومصدر الرعاية

إلى الذي لا يسعني إلا أن أقف أمامه وقفة احترام وعرفان وحسب...

إلى الذي تمنيت لو أنه حضر يوم تخرجي....لكن ....إنا لله وإنا إليه راجعون...

إلى أبي الغالي و أخي وصديقي ...دحمان...رحمه الله وأسكنه فسيح جنانه بإذنه تعالى

فيا رب اجمعني و إياه في جنانك جنان النعيم

إلى القلب الدافئ والصدر الرحيب"والدتي الغالية..."أم الخير" ...حفظها الله ورزقني الله برها وأكرمني برضاها.

إلى ذكريات الطفولة و أمن المستقبل "أشقائي وشقيقتي" حفظهم الله تعالى.

إلى الكتاكيت الصغار " هشام""سمير""بيبي"أماني"ياسين""عبدو"

إلى أخوالي وخالاتي وخاصة خالتي "ربيحة"

إلى أعمامي وعمتي

إلى جدتي أطال الله في عمرها

إلى أخي و صديقي وحبيبي الذي صبر عني والذي شاركني أعباء هذا العمل و تحمل وزري"كيمو"

إلى أصدقائي الذين كانوا إخوتي الذين لم تلدهم أمي كل باسمه"السعيد- نصرو- يعقوب- بوليسي- نوري- رضا- رحيم- عماد- وليد- فتحي- حمزة- ياسين- حميد- يوسف- رشدي- عزوز- عادل- بلال- محمد- عزيز- علي- يوسف..."

إلى زميلاتي"ايمان- فيروز- خديجة- فايزة- عبلة- سلمى- حنان- أسماء- وهيبة- خضرة- فيفي..."

إلى الكريمة في ودها و الصديقة في إخلاصها و الرفيقة و الشريكة في أمانتها و العزيزة في حبها ،إلى من اختارها قلبي شريكة له في الحياة إلى..حنان..

إلى كل من يقول لا إله إلا الله

محمد



إهداء

إلى ينبوع الرحمة والحنان ومصدر العطاء والوفاء، إلى التي شقت من أجل سعادتي واشترت راحتي بتعبها وشقائها إلى أغلى اسم نطقه لساني إلى روح الفقيدة الطاهرة أمي

إلى من كان لي بمثابة الشمعة التي تحترق لتنير طريقي إلى الذي كانت نصائحه وتوجيهاته دربا منيرا أهتدي به وكان دائما نعم المثل ونعم القدوة أبي

إلى من قاسمتهم معنى الحياة فكانوا سندا لي إخوتي: نور الدين، سليم

إلى أخواتي وأزواجهن وأبناءهم: مريم، أيمن، شمس الدين،والصغيرة مروى

إلى أبناء عمي: سمير ، حليم، إلى كل من لقب ذياب و قدوج.

إلى إخوتي الذين لم تلدهم أمي: فيصل بلال هشام محمد زينو فواز ياسين عبد الرزاق حليم نبيل خير الدين عمار. وليد.عبد الرحيم.

إلى من قاسمني أعباء هذا العمل أخي محمد .

إلى من قضيت معهم أجمل أيام الجامعة وأحمل لهم في قلبي مشاعر الحب والخير والطيبة: السعيد 30 بوليسي12 نصرو 19 النوري12 ميدا12 سليم 12 باديس43 عماد40 رضا12 وليد 19عزيز18 بكيري 12 زاكي 18 الزاوش28 يعقوب05 إلى كل طلبة الدفعة 2008. وخاصة الطيب أيمن كريم فتحي فوزي

إلى كل الزملاء والزميلات في الدراسة كما أهدي هذا العمل إلى كل الأهل: الأعمام و الأخوال.

إلى كل من علمني حرفا أساتذتي في جميع مراحل الدراسة .

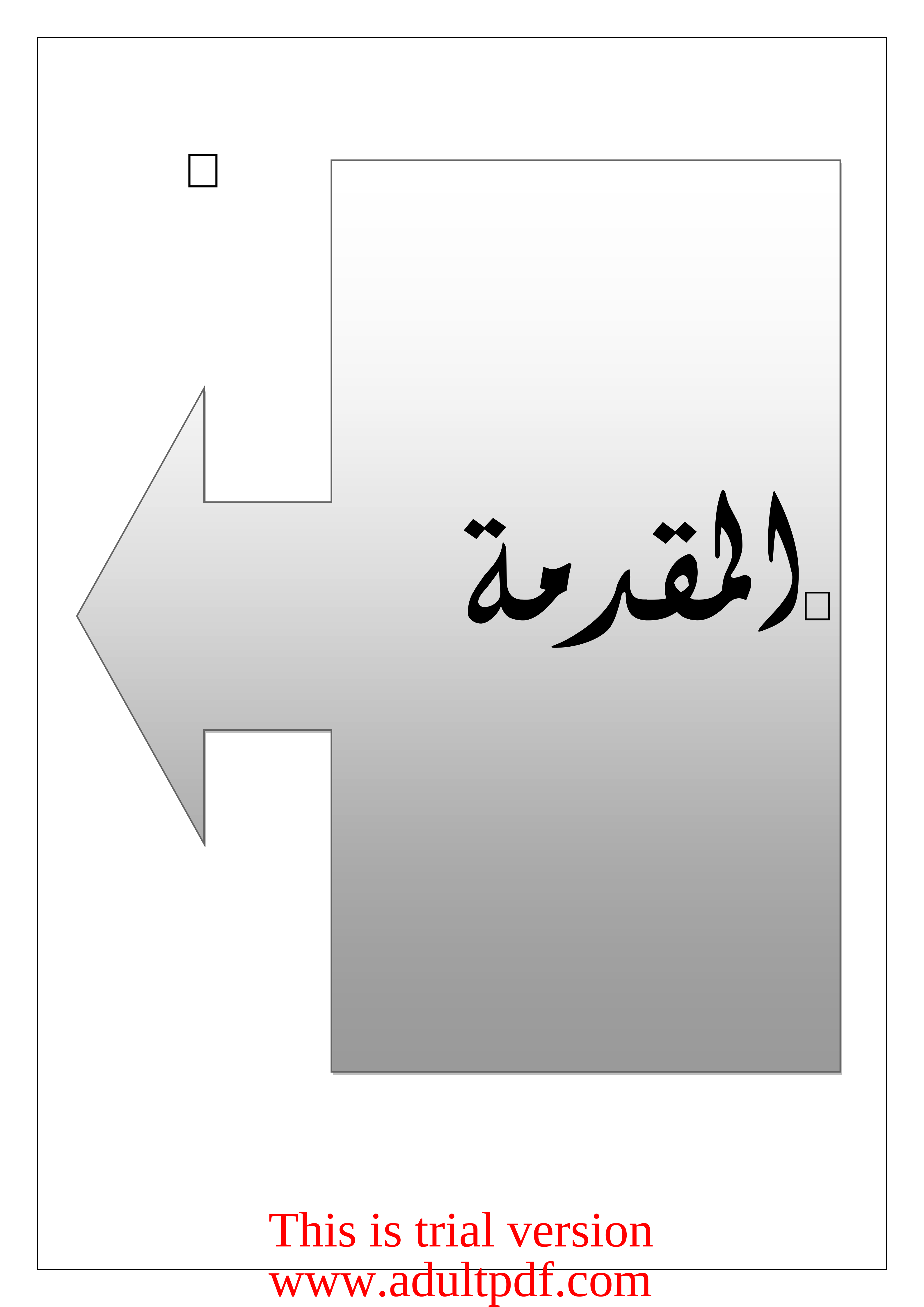
إليك أنت يا من تقرا هذا الإهداء.

قائمة المحتويات:

➢	شكر وتقدير	
➢	إهداء	
➢	خطة البحث	
➢	قائمة المختصرات	
➢	المقدمة	أ - م
➢	**الفصل الأول: ماهية مواقع الويب وخصائصها**	
	تمهيد	**16**
1-1	**ماهية المواقع**	**16**
1-1-1	مفهوم المواقع	**16**
2-1-1	أنواع المواقع	**16**
3-1-1	أهداف المواقع	**17**
4-1-1	أهمية مواقع الويب	**18**
5-1-1	مميزات المواقع	**18**
2-1	**تصميم صفحات المواقع**	**19**
1-2-1	أدوات البرمجة	**19**
2-2-1	برمجيات تصميم المواقع	**20**
1-2-2-1	برمجية Microsoft Frontpage	**20**
2-2-2-1	برمجية Home site	**20**
3-2-2-1	برمجية ..Web Publisher	**20**
3-1	**لغات تصميم المواقع**	**21**
1-3-1	لغة النصوص الفائقة HTML	**21**
2-3-1	لغة الجافا JAVA	**21**
4-1	**معايير تقييم المواقع**	**22**
5-1	**دور المواقع في خدمة الباحث و البحث العلمي**	**24**
	خلاصة	**25**
	الفصل الثاني: عناصر التهديد الأمني للمعلومات الالكترونية	
	تمهيد	**28**
1-2	**تعريف التهديدات الأمنية**	**28**
2-2	**أنواع التهديدات الأمنية**	**29**
3-2	**أسباب التهديدات الأمنية**	**30**
4-2	**المجرم المعلوماتي**	**30**
1-4-2	الهاكرز	**31**

31	الكراكرز	2-4-2
31	الفرق بين الهاكرز و الكراكرز	3-4-2
32	**الفيروسات**	5-2
33	أنواع الفيروسات	1-5-2
33	أشهر الهجمات الفيروسية(نماذج من فيروسات المعلومات)	2-5-2
34	الديدان الفيروسية	3-5-2
35	برامج ذاتية التحميل وأحصنة طروادة	4-5-2
35	برامج ذاتية التحميل	1-4-5-2
36	أحصنة طروادة(trojan horses)	2-4-5-2
37	**كيفية الاختراق**	6-2
38	**عملية تشويه موقع ويب**	7-2
39	**خلاصة**	
	الفصل الثالث: أمن وحماية معلومات المواقع الإلكترونية	
42	**تمهيد**	
42	**تعريف أمن المعلومات**	1-3
42	**أهمية أمن المعلومات**	2-3
43	**أشكال الحماية الالكترونية**	3-3
43	البرامج المضادة للفيروسات	1-3-3
43	مفهومها	1-1-3-3
43	تشغيل البرامج المضادة للفيروسات	2-1-3-3
44	برامج جدران النار	2-3-3
45	ملقمات الانترنت	3-3-3
45	التشفير (Encryptions)	4-3-3
47	**برتوكولات أمن المعلومات**	4-3
48	**خطوات أمن المعلومات**	5-3
49	**دور الجامعات والمعاهد العلمية في تطوير آلية التعامل مع النظم المعلوماتية**	6-3
50	**خلاصة**	

الفصل الرابع: إجراءات الدراسة الميدانية		
تمهيد		53
1-4	تحليل البيانات و تفريغها	54
2-4	النتائج العامة للدراسة	65
3-4	النتائج العامة على ضوء الفرضيات	66
4-4	الاقتراحات	68
➢ خاتمة		70
➢ قائمة المراجع		
➢ الملاحق		
➢ الملخصات		


المقدمة

مقدمة :

إن السعي المتواصل لبلوغ درجة الأفضلية واكبته حركة هائلة في مجال المعلومات و نشرها، إذ لم تصل البشرية إلى مطلع الستينات من القرن الماضي حتى وجدت نفسها تتخبط في سيل عارم من المعلومات، وهو ما أدخلها في دوامة مجهولة المعالم،أساسها المعلومات و ما أصطلح عليه بثورة المعلومات أو الانفجار المعلوماتي، لكن و بالموازاة مع ذلك كانت بعض الدول تسعى لفرض سيطرتها على العالم سياسيا و اقتصاديا ،ما نتج عنها نشوب الحربين العالميتين الأولى و الثانية، إذ ما فتأت تنتهي حتى تمخضت عنها صراعات أدت هي الأخرى بدورها إلى ظهور الحرب الباردة، هذه الظاهرة استقطبت اهتمام العديد من الهيئات التي سعت بدورها إلى إنتاج أساليب ووسائل تمكنها من الصعود إلى مرتبة القيادة فأدت إلى بروز ظاهرة الانترنت التي تطورت مع مرور الوقت إلى أن وصلت إلى ما هي عليه الآن من التطور و العالمية التي لا تحكمها قوانين ولا تحدها حدود أو حواجز.

و في مجتمع الفضاء السيبيري – ذلك النسق الهائل لترتيب و إتاحة كميات ضخمة من المعطيات في الحاسب- تحول العالم إلى بيت عنكبوت غير منظم الروابط عالم الشبكات و الصفر و الواحد، موصولة بطريقة افتراضية وفضائية فائقة السرعة،عالم توحدت فيها لبنى التحتية المعلوماتية على المستويات الوطنية و الإقليمية و الدولية لتصبح بنية معلومات كونية، عصر وصلت فيه التطورات الرئيسية كما وصفها "كاكو" في أعمدة العلم الثلاثة: <المادة-الحياة-العقل> <<الذرة-الـ ADN –الحاسب>> إلى قمتها، عصر أصبح فيه الخيال العلمي واقعا بل أصبح من الصعب التفريق بين الواقع و الخيال واقع تغيرت فيه قواعد اللعبة السياسية ،عالم يتشكل و يعاد تشكيله بسرعة، عصر حروبه بلا جيوش وبلا دماء أستبدل فيه الرصاص بالبيانات فلم تعد الحكومات تخشى من بعضها بقدر خشيتها من المنظمات و الأفراد و المجموعات.

لقد أدت تكنولوجيا الاتصالات إلى ظهور الشبكات و قواعد المعلومات التي أصبحت تقدم أحدث المعلومات في ثوان، لذا فعلى كل مؤسسة علمية أرادت النجاح في تقديم خدمات أفضل أن تتبنى هذه التقنيات و التكنولوجيات بما فيها مواقع الويب، و بالتالي توافد جمهور المستفيدين إليها و سعيهم وراء الاستفادة من خدماتها، فقد أصبحت هذه التكنولوجيا تشكل حجر الأساس داخل محيط البحث العلمي بالجامعات و مؤسسات التعليم العالي لما تتيحه من فرص تأمين الوصول إلى المعرفة بجميع أشكالها و أنواعها.

ولقد أدت الثورة التي أنتجتها المعلومات في العقدين الأخيرين إلى قلب الموازين و إحداث تغيرات جذرية في المفاهيم وفي علاقات الناس، وإذا كان من

عامل مشترك لكل هذه التحديات فإنه يمكن تلخيصه في كلمة واحدة و هي المعلومات؛ ذلك المصدر الهام و النادر، سلاح الهجوم و سلاح الدفاع، وكما أن هذا العالم الجديد أصبح يزخر بانتصارات تنير درب البشرية فإن له كذلك جانباً مظلماً،حيث فتح المجال فيه للعبث و الجريمة في احدث ثوب لها ، فقد أصبحت جرائم المعلومات و أنظمتها بلا حدود فهي جرائم عالمية و التحقيق فيها و الحكم عليها عملية معقدة، وترتكب هذه الجرائم من قبل الأفراد و المجموعات على حد سواء، كما يمكن أن ترتكب من طرف مراكز البحوث و الأكاديميي ن كما ترتكب من طرف أشخاص عاديين.إنه العالم السفلي للانترنت عالم له مسيروه ومطوروه و رواده.

كتب الفقيه الفرنسي "ميلر- MELLOR" في عام 1972:"إن الكمبيوتر بشراهته في جمع المعلومات على نحو لا يمكن وضع حد لها، وما يتصف به من دقة ومن عدم نسيان ما يخزن فيه، قد يقلب حياتنا رأساً على عقب؛ يخضع فيها الأفراد لنظام رقابة صارم و يتحول المجتمع بذلك إلى عالم شفاف تصبح فيه بيوتنا و معاملاتنا المالية و حياتنا العقلية و الجسمانية عارية لأي مشاهد".

ولو كان يعرف "ميلر" ما ستؤول إليه فتوحات عصر المعلومات، وما سيتحقق في بيئة شبكات المعلومات العالمية و العالم الالكتروني لأدرك أن ما قاله أصبح يسيراً على التقنية، فهي فيما وصلت إليه الآن من مراحل التطور أمكنها أن تجمع شتات المعلومات عن كل فرد و تحيلها إلى بيان تفصيلي بتحركاته و هواياته و مركزه المالي و غيرها.

ولأن الخطر تعاظم باستخدام وسائل الكشف و المعالجة التقنية، كان لزاماً أن تظهر وسائل تقنية أيضاً لمواجهة هذا الخطر، لكن سنبقى نذكر أن الحماية عبر الوسائل التقنية تجيء لاحقة على المخاطر و الاختراقات التقنية لهذا تظل المخاطر أسبق في الحصول و تظل الحماية في موضع متأخر عنها.

و لمعالجة موضوع البحث، تم تقسيم الدراسة إلى أربعة فصول جاءت على النحو التالي:

الفصل الأول: و الذي جاء تحت عنوان " ماهية مواقع الواب و خصائصها " فقد يتم التطرق من خلاله و بإسهاب إلى ماهية المواقع الالكترونية من خلال تبيان أهم خصائصها وأهدافها وكذا أنواعها، كما كيفية تصميم صفحات مواقع الويب وأهم البرمجيات المستعملة فيها دون أن ننسى مميزاتها و دورها في خدمة الباحث و البحث العلمي عامةً.

الفصل الثاني: فقد تناولنا فيه التهديدات الأمنية للمواقع الالكترونية من خلال التطرق إلى الأسباب المؤدية لهذه التهديدات بالإضافة إلى المجرم المعلوماتي من

خلال معرفة أهم أنواع وأنماط المجرمين و الفرق بينهم، وكذا الأسباب التي تدفعهم إلى هذه الجرائم،مع ذكر أهم الفيروسات وكيفية اختراقها و أنواعها.

الفصل الثالث: و الذي جاء تحت عنوان : أمن وحماية معلومات المواقع الالكترونية، فقد تعرضنا إلى أمن المعلومات هذه المعضلة التي حياة الأفراد و الجماعات، وكذا أشكال الحماية الالكترونية و البرامج المضادة للفيروسات، كما تطرقنا إلى بروتوكولات وخطوات أمن المعلومات .

الفصل الرابع: تفريغ البيانات و تحليلها، ويتعلق الفصل بالدراسة الميدانية التي أجريت -كما ذكرنا سابقا- على موقع جامعة منتوري قسنطينة حيث تناولنا فيه تحليل وتفسير بيانات المقابلة و النتائج على ضوء الفرضيات و النتائج العامة للدراسة.

ولإنجاح هذه الدراسة و الإحاطة بمختلف جوانبها تمت الاستعانة بمجموعة من المصادر و الوثائق محاولين توظيفها كلها في مختلف عناصر الفصول المتوفرة لدينا، غير أننا لم نخوض داخل هذا المقام أكثر بل سنذكر البعض منها فقط وهي:

- ✓ داوود، حسن الطاهر.الحاسب وأمن المعلومات، الرياض: مكتبة الملك فهد الوطنية .2000
- ✓ الحميد، محمد دباس.حماية أنظمة المعلومات، عمان: دار الحامد للنشر و التوزيع،2007
- ✓ صادق، دلال.أمن المعلومات،عمان :دار اليازوري العلمية،2008
- ✓ البداينة، ذياب.الأمن و حرب المعلومات،الأردن: دار الشروق،2002

و في الأخير نود الإشارة إلى أنه أثناء إعدادنا لهذا العمل المتواضع واجهتنا مجموعة من الصعوبات نذكر منها على سبيل المثال لا الحصر :

- كثرة المراجع التي عالجت الموضوع من زوايا متعددة، مما شكل لنا حاجزا نفسيا في عملية انتقاء المناسب منها بما يتناسب مع موضوع بحثنا، خاصة أنه يتطرق إلى الموضوع من زاوية لم نجد الموافق منها ضمن ما توفر لدينا من أوعية فكرية.

- ضيق الوقت المخصص لإعداد المذكرة.

و للوقوف على حيثيات الموضوع ارتأينا إتباع الإطار المنهجي التالي :

1-الإشكالية:

إن نمو وتقدم المجتمعات الحالية أصبح يقاس بمدي ثقافة وتعلم أفرادها ولذلك وجب عليها اعتماد سياسة وطنية حكيمة من أجل تكوين وتدريب أفرادها من خلال إنشاء مؤسسات ومراكز تعليمية لهذا الغرض، و الجامعة الجزائرية كواحدة من هذه

المؤسسات تعتبر مركز إشعاع علمي تسعى إلى تقديم وتكوين إطارات قادرة على النهوض بالأمة من خلال الإمكانات والخدمات التي تضعها الدولة تحت تصرفها من أجل السير الحسن ودوام إستمراريتها، ودورها في المجتمع كان لابد عليها أن تعمل على التواصل مع العالم الخارجي خاصة الجامعات العالمية الكبرى لتبادل الأفكار و الخبرات يما بينها .

وعلى هذا الأساس ونظرا لتطور التكنولوجيا والاتصال وظهور شبكة الانترنيت كواحدة من أهم اكتشافات العصر الحالي والتي ساهمت وبشكل كبير في تقليص البعد الجغرافي بين مختلف الجامعات العالمية والوطنية فقد ارتأت الجامعة الجزائرية من خلالها مواكبة التطور التكنولوجي من خلال إنشاء مواقع إلكترونية خاصة بها يتم وضع كل المعلومات المتعلقة بها والنشاطات التي تقوم بها.

ولكن وفي ظل ظهور وتطور الجريمة المعلوماتية بكل أنواعها وأشكالها التي تهدد أمن المواقع إلكترونية وخاصة منها المهمة والحساسة ،فقد أصبحت التهديدات الأمنية الهاجس الأوحد والدائم للجامعة الجزائرية خاصة ونحن نعلم أن المواقع هي نافذتها الإعلامية على العالم ،ونظرا لأهمية مبدأ تحقيق أمن تلك المعلومات فإنه لابد من توخي الحذر واعتماد أساليب الوقاية من كل ما من شأنه أن يكون تهديدا أمنيا للموقع الإلكتروني ككل وبالمعلومات المنشورة بداخله على وجه الخصوص لهذا أصبح لزاما على الجامعة التفكير و السهر على إيجاد حلول وطريقة فعالة لحماية مواقعها من أي خطر مرتقب من طرف مجرمي الانترنيت وضمان استمرارية عملها ومن هنا يمكن طرح التساؤل الرئيسي التالي:

ما طبيعة التهديدات الأمنية التي تهدد المواقع الإلكترونية للجامعة الجزائرية وطرق حمايتها؟

التساؤلات الفرعية:

- ما هي أهم المخاطر التي تواجه أمن المواقع الالكترونية في ظل تسارع وتطور نظم الاختراق و القرصنة

- ما هي الآثار السلبية لتلك التهديدات الأمنية على الموقع الالكتروني لجامعة منتوري؟

- هل أصبحت البيئة الالكترونية أقل أمنا و عرضة لانتهاكات الأفراد و العصابات ؟

- كيف يمكن الوقاية والتقليص من حجم تلك التهديدات الأمنية ؟

2- الفرضيات:

و لمعالجة ما جاء ضمن التساؤلات و الوقوف على واقع الظاهرة المدروسة تمت صياغة الفرضية الرئيسية التالية :

تتوقف حماية المواقع الالكترونية للجامعات الجزائرية من التهديدات الأمنية على مدى تبنيها لطرق حماية ناجعة.

و من هذا المنطلق تم صياغة فرضيات جزئية كما يلي :

- سبل الحماية و الوقاية المتوفرة داخل المواقع الالكترونية كفيلة للحد من التهديدات الأمنية والتصدي لها.
- تتفاوت انعكاسات التهديدات الأمنية على محتويات المواقع الالكترونية بحسب طبيعة تلك المحتويات.
- ضعف أنظمة الحماية داخل المواقع الالكتروني ة يجعلها أكثر عرضة للتهديدات الأمنية.

3- المنهج المعتمد في الدراسة :

يعتبر المنهج ضرورة في أي بحث علمي، فهو الطريقة المثلى التي يمكن بفضلها الإجابة على السؤال المطروح ألا وهو : ***ما مدى تأثير التهديدات الأمنية على المواقع الالكترونية للجامعة الجزائرية؟***

إذن فالمنهج هو: "مجموعة من القواعد العامة المصوغة من أجل الوصول إلى الحقيقة في العلم".[1]

إن طبيعة موضوع الدراسة وخصائصها هي التي تحدد المنهج المستخدم ، وبما أن دراستنا تقوم على وصف تأثيرات التهديدات الأمنية على المواقع الالكترونية استخدمنا المنهج الوصفي، حيث يقوم هذا الأخير "بوصف الظواهر الطبيعية و الاجتماعية كما هي ، وهو مكمل لمنهج التاريخي الذي يصف الظواهر في تطورها الماضي حتى يصل بها إلى الوقت الحاضر ، و المنهج الوصفي لا يقوم بوصف الواقع كما هو، و إنما يصفه بطريقة انتقائية أو اختيارية، فهو يختار من الواقع الماثل أمامه، وينتقي منه ما يخدم غرضه من الدراسة".[2] ومن ثمة فإن المنهج الوصفي لا يقوم فقط على وصف الظاهرة كما هي ، بل يتعداه إلى جمع البيانات و المعلومات وتصنيفها و تحليلها.

4- عينة الدراسة :

تعرف العينة بأنها هي العملية الرامية إلى تحديد العينة الممثلة لمجتمع الدراسة والذي يكون لمجموع أفراده علاقة بموضوع البحث.

و بالنظر لطبيعة موضوع الدراسة و المتعلقة ب : التهديدات الأمنية للمواقع الالكترونية للجامعة الجزائرية، اعتمدنا العينة العمدية و المتمثلة في شخص القائم على موقع الجامعة مجال الدراسة، باعتباره الشخص الأنسب و الوحيد الذي بإمكانه إعطاء كل المعلومات المتعلقة بالموضوع.

[1] - عليان، ريحي مصطفى؛***غنيم عثمان محمد.أساليب البحث العلمي:الأسس النظرية و التطبيق العلمي***،(ط.2)،عمان:دار صفاء للنشر و التوزيع. 2008،ص.22.

[2] - الضامن ، منذر، ***أساسيات البحث العلمي***.(ط.1)، عمان : دار المسيرة للنشر و التوزيع، 2009 ، ص.28.

5- أسباب اختيار الموضوع:

من بين الدوافع التي أدت بنا إلى طرق هذا الموضوع هو محاولة إلقاء الضوء على هذا العالم الغامض و المثير، و التعريف بأهمية توفير الحماية لمعلومات الأفراد وخصوصياتهم، ويمكن تلخيص أهم هذه الأسباب فيما يلي:

- محاولة تسليط الضوء على الجوانب الغامضة في البيئة الالكترونية من الناحية التقنية و انعكاساتها على حياة الأفراد.
- محاولة قياس قدرة المواقع الالكترونية على حماية معلوماتهم ومدى اطلاعهم على مختلف أساليب الحماية.
- محاولة معرفة مدى تطور أنظمة الحماية داخل المواقع الخاصة بالجامعات الجزائرية.
- محاولة معرفة أهم الأخطار التي تتربص بالمواقع الالكترونية للجامعات الجزائرية.
- الرغبة الشخصية في مثل هذه المواضيع لما تكتسيه من حداثة و ارتباطها الوثيق بالتخصص.

6- أهمية الموضوع:

في عصر الازدهار الالكتروني وفي زمن قيام الحكومات الالكترونية، زمن القرية الكونية، تبدل نمط الحياة وتغيرت معه أشكال الأشياء و أنماطها ومنه لا شك من تبدل أنماط المجرمين وكذا أنواع جرائمهم والتي قد يحتفظ بعضهم باسمها التقليدي القديم مع تغير جوهري في طرق ارتكابها، إذن نقف اليوم على أعتاب حضارات وثقافات جديدة،حيث تضمحل وتزول كل الحواجز و الحدود ،ثقافات رسمت معالم لمصطلحات من هذه البيئة.

إن انتشار التكنولوجيا الحديثة واستعمالاتها التي مست كل منا في الحياة، أفرزت العديد من التحولات و التغيرات و المخاطر و الوسائل و التقنيات بشقيها الإيجابي و السلبي، فغذت على أعتابها البيئة الجديدة مسرحاً للعديد من التناقضات و التحولات و التحديات على الصعيد التقني وعليه ارتأينا الخوض في غمار هذا العالم الكبير و الواسع و اكتشاف خباياه وتسليط الضوء على بعض جوانبه.

- محاولة استطلاع الواقع عن قرب لمعرفة مدى تمكن الموقع الالكتروني لجامعة منتوري-قسنطينة- من مواجهة مجرمو الانترنت و المعلومات و كذا مجابهة الفيروسات وكيفية حمايته من هذه الأضرار.

- الاهتمام الشخصي بالموضوع و ما له علاقة بعالم الإعلام الآلي و التقنية الحديثة.

7- أهداف الدراسة:

نهدف من وراء هذه الدراسة في مجال أمن المعلومات و الجريمة الالكترونية إلى:

*من الناحية النظرية محاولة تجميع مختلف جوانب الموضوع و المشتتة في العديد من المراجع و جمعها في عمل واحد بغرض خدمة البحث العلمي.

*معرفة آخر ما توصلت إليه التكنولوجيات الحديثة في مجال الجريمة المعلوماتية و أمن المعلومات.

*أما الجانب الميداني من البحث فيهدف إلى :

- معرفة أنظمة الحماية المنتهجة في موقع جامعة منتوري قسنطينة.

- معرفة أهم التهديدات الأمنية التي تهدد أمن موقع جامعة منتوري –قسنطينة.

8- أدوات جمع البيانات :

إن طبيعة الموضوع هي التي تفرض على الباحث نوع الأدوات التي يستخدمها في جمع بيانات حقل موضوع الدراسة، إذ أن الوصول إلى نتائج أكثر دقة يتوقف على مدى التحكم في هذه الأدوات و التي تتطلب عناية كبيرة من طرف الباحث.

ومن بين الأدوات التي اعتمدنا عليها في جمع المعلومات المتعلقة ببحثنا هي :

- <u>المقابلة:</u> تعتبر المقابلة أداة أساسية في جمع البيانات و المعلومات :" حيث تشتمل على أسئلة محددة للحصول على إجابات دقيقة بشأنها ، فالباحث يتحاور مع الإنسان الذي يجري معه المقابلة، و يغير أسلوب الأسئلة إذا كان هناك بعض الغموض"[1].

ونظراً لطبيعة الوصفية لدراستنا ، فقد استخدمت المقابلة المحددة الأسئلة مع السيد المشرف على امن موقع جامعة منتوري كونه الشخص الوحيد الذي بإمكانه تزويدنا بما نحتاجه من معلومات وخاصة أنه هو المسؤول المباشر على حماية الموقع، وبيان المقابلة الذي يحتوي على الأسئلة موجود في الملاحق.

وقد ضمنا في المقابلة مجموعة من الأسئلة عددها 26سؤال، 09 أسئلة متعلقة بالعنصر الذي يدور حول سبل الحماية و الوقاية المتوفرة داخل المواقع الالكترونية

---

[1]- غربي ، علي . ***أبجديات منهجية في كتابة الرسائل الجامعية***. قسنطينة : Cirta Copy ، 2008 ،ص.22.

كحيلة بلحد من التهديدات الأمنية والتصدي لها. 10، أسئلة تتعلق بالعنصر الذي يعنى بتفاوت انعكاسات التهديدات الأمنية على محتويات المواقع الالكتروني، 07 أسئلة تتعلق بضعف أنظمة الحماية داخل المواقع الالكترونية.

9- مجالات الدراسة:

تتسم الدراسات الميدانية بجملة من المجالات، من شأنها تحديد أبعاد الدراسة من حيث البعد الجغرافي، المجال الزمني و أخيرا المجال البشري.

المجال الجغرافي:

لقد قمنا بإجراء الدراسة الميدانية بجامعة منتوري –قسنطينة- و التي تقع في الجهة الشرقية الجنوبية لولاية قسنطينة و التي تبعد عن مقر الولاية بحوالي 05كلم وتحتل موقعاً استراتيجياً هاماً يجذب كل الناظرين وهي تتوسط شبكة المواصلات مما يسهل الوصول إليها من كل مكان.

في سنة 1968 وضع الرئيس الراحل "هواري بومدين" حجر الأساس لميلاد جامعة منتوري –قسنطينة- ولقد صمم هيكلها البرازيلي "نميار- Nemeyer" بحيث كانت الانطلاقة الفعلية لنشاط الجامعة في سنة 1970 و التي أصبحت فيها جامعة قسنطينة مستقلة، بعدما كانت تابعة لجامعة الجزائر.

كان موقع جامعة منتوري- قسنطينة – الالكتروني الواقع مقره بالطابق الرابع عشر في البرج الإداري هو المجال الجغرافي للدراسة، هو موقع حديث النشأة حيث كان ذلك في 01 فيفري 2007 ثم تلته الطبعة الثالثة و الحالية و التي أنشأت من طرف السيد :"بلبكري عادل" وهو المسؤول عن الموقع، وقد تم ذلك بتاريخ 2010/02/01،[1] كان هو مجال إجراء الدراسة و التي تضمنت مجموع التساؤلات التي تضمنتها الإشكالية، و ما تفرع عنها من فرضيات. وقد تمت صياغة الفرضيات على النحو التالي:

سبل الحماية والوقاية المتوفرة داخل المواقع الالكترونية كحيلة بلحد من التهديدات الأمنية والتصدي لها.

تتفاوت الانعكاسات للتهديدات الأمنية على محتويات المواقع الالكترونية بحسب طبيعة تلك التهديدات.

ضعف أنظمة الحماية داخل المواقع الالكترونية يجعلها أكثر عرضة للتهديدات الأمنية.

المجال البشري:

---

[1] -WWW.UMC.EDU.DZ/VF/INDEX.PHP/WEBMASTER

و قد تشكل الإطار البشري من السيد المشرف على موقع الجامعة مجال الدراسة و الذي تمت معه المقابلة التي تضمنت 26سؤال، و كان ذلك يوم 13 مارس 2011 من الساعة.... الى الساعة

المجال الزمني :

نحدد وكما هو معروف في المجال الزمني مراحل سير المذكرة، المتعلقة بطبيعة الموضوع ونوعية الدراسة و الإمكانيات المتوفرة لإنجاز البحث، وعلى هذا الأساس تنحصر مراحل إنجاز بحثنا في ثلاث مراحل وهي:

أ-المرحلة الأولى : قبل الحديث عن هذه المرحلة تجدر بنا الإشارة إلى أننا في أول الأمر قد كنا اخترنا هذا الموضوع و لكن بدراسة موسعة وذلك من خلال عدة مواقع جامعات مختلفة بالشرق الجزائري،لكن ونظراً لضيق الوقت وكذا الإجراءات المفروضة علينا من طرف الإدارة ، ولهذا اكتفينا بموقع واحد ألا وهو موقع جامعة منتوري-قسنطينة- وذلك بعد زيارتنا لمقر هذا الأخير الكائن بالبرج الإداري بالجامعة المركزية، وكان ذلك يوم 13 مارس 2011 ، حيث توجهنا إلى الطابق الرابع عشر بالبرج الإداري عند السيد المشرف على حماية وأمن الموقع،الذي رحب بنا واستحسن الفكرة وأعرب عن استعداده لمساعدتنا ، ومن بعد أن طرحنا عليه الموضوع قدم لنا لمحة بسيطة عن الموقع وكيفية عمله وبعض الشروحات الهامة.

وقد كان من الصعب تحديد المراجع لأن الموضوع واسع جداً ويتطلب الكثير من التركيز و الوقت وتتوفر فيه الكثير من المصادر و المراجع لا يمكن الاعتماد عليها كلها، وقمنا بتحديد مجال الدراسة لأنه كما ذكرنا سابقاً أن موضوع الدراسة واسع وله جوانب عديدة ، منتقلين فيما بعد إلى تحديد الإشكالية.

ب-المرحلة الثانية : وبناءاً على ما تم بناءه في المرحلة السابقة وبعد تحديد الإشكالية و أسبابها ،انتقلنا إلى تأسيس الجانب النظري من الدراسة و الذي يتضمن ثلاث فصول ؛ الفصل الأول حول ماهية المواقع الالكترونية ودورها في خدمة البحث العلمي ، و الفصل الثاني حول التهديدات الأمنية والفصل الثالث يتعلق بأمن المعلومات الالكترونية. وهذا طيلة أشهر مارس؛ أفريل و ماي وطالت هذه المدة لصعوبة اختيار المراجع التي تخدم الموضوع.

المرحلة الثالثة : في نفس الوقت الذي تم فيه بناء الجانب النظري تم التحضير للجانب الميداني ، حيث تم إجراء مقابلة مع السيد المشرف على أمن موقع جامعة منتوري و ذلك يوم الاثنين 11 أفريل 2011 و هذا الجزء الأول ، وقد تم إكمال الجزء الثاني لتأخذ شكلها النهائي بعد أسبوع أي يوم 18 أفريل 2011 ، لنتفرغ بعد ذالك إلى تحليل البيانات و تفسيرها حتى بداية شهر جوان ، وفيها بعد انتقلنا إلى عملية الطباعة في أوائل شهر جوان ، لتخرج في شكلها النهائي الذي هي عليه الآن.

10- تحديد مفاهيم الدراسة :

- مفهوم المواقع : يمكن تعريف موقع الويب بأنه عبارة عن صفحة ويب واحدة أو أكثر يقوم بإعدادها شخص أو شركة تكون مسؤولة على محتوى المواقع الخاص بها.[1]

- مفهوم التهديدات الأمنية : يعرفها مكتب المحاسبة بالولايات المتحدة الأمريكية بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"

- مفهوم أمن المعلومات : فإن أمن المعلومات هو مجموعة الخطوات التي تهدف إلى حماية الحاسوب والمعلومات المخزنة داخله من الاختراقات والفيروسات وغيرها من عناصر التهديد الأمني للمعلومات من خلال مكافحة ملفات التجسس وحماية المعلومات الخاصة الشخصية.[2]

11-الدراسات السابقة :

1-الدراسة الأولى: [بن ضيف الله، فؤاد] 3

و التي تعتبر دراسة لها علاقة وطيدة ببحثنا حيث تطرقت إلى الجوانب المتعلقة بمعلومات البيئة الالكترونية وأمن المعلومات داخل هذه البيئة.

2-الدراسة الثانية: [شوقي، حسام] 4

وهي دراسة شاملة تمس موضوع المذكرة،وقد تطرق المؤلف بشيء من الإيجاز إلى مختلف الجوانب التي تعالج موضوع شبكة الانترنت وتوفير الأمن سواءُ للبريد الالكتروني أو للمعلومات المتاحة في الشبكة،كما تعرض إلى الاختراق أساليبه وبرمجياته.

3-الدراسة الثالثة: [الجنيهي، منير محمد] 5

حيث يخوض في غمار التشريعات القانونية في محاربة و مكافحة الجرائم الحديثة.

---

[1] -Voss,Andrés. ***Dictionnaire de l'informatique et de l'anterret*** 1999 paris: micro .application 1998,p.502

[2] أمن المعلومات. [متاح على خط]: . ***URL:safola.Com/security. chtml.*** تمت الزيارة يوم:2011/02/10

[3]- بن ضيف الله، فؤاد. ***أمن المعلومات و حقوق التأليف الرقمية.*** مذكرة ماجستير: علم المكتبات : قسنطينة، جامعة منتوري :2002

[4]- شوقي، حسام . ***حماية وأمن المعلومات على الانترنت.***القاهرة:دار الكتب العلمية،2003

[5]- الجنيبيهي، منير محمد ؛ الجنيبهي ممدوح محمد ، ***جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها.*** الاسكندرية: دار الفكر العربي ،2004 .

4-الدراسة الرابعة: [البداينة، ذياب] 1

وقد عالج فيها العديد من القضايا التي تخص الأمن الوطني من منظور معلوماتي وكيفية حماية الكيانات المعرفية في الفضاء الافتراضي و الذي أصبح عرضة لانتهاكات و أخطار لا متناهية، كما تطرق إلى خصائص المجرمين المعلوماتيين وأنواعهم ومختلف مميزاتهم و أسبابهم للجريمة.

[1] - البداينة، ذياب. ***الأمن وحرب المعلومات***. عمان : دار الشروق للنشر و التوزيع.2006

5-الدراسة الخامسة: [سعيدي، سليمة] 1

سعيدي سليمة "الهاكرز وأمن المعلومات"وهي دراسة متعمقة تمس موضوع بحثنا مباشرة فقد عالجت العديد من الجوانب للمجرم المعلوماتي و الفيروسات وكيفية توفير سبل الحماية و الوقاية من الهاكرز و الكراكرز(المخترقين).

6-الدراسة السادسة: [غزال، عبد الرزاق] 2

غزال عبد الرزاق "أمن المعلومات الالكترونية وحقوق المؤلف في ظل التشريع الجزائري" وقد عالج في هذه المذكرة القضايا التي تخص أمن المعلومات داخل البيئة الالكترونية من الناحية التشريعية أي الملكية الفكرية وحقوق المؤلف الرقمية المتعلقة بالمصنفات الرقمية.

7-الدراسة السابعة: [صادق، دلال] 3

دلال صادق"أمن المعلومات" حيث عالج هذا المؤلف في هذا الكتاب أساليب مواجهة تهديدات أمن المعلومات وتحليل المخاطر الناجمة عن الانتهاك و الاختراقات و أيضاً العقبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية.

8-الدراسة الثامنة: [دباس الحميد، محمد] 4

محمد دباس الحميد "حماية أنظمة المعلومات" حيث تناول المؤلف موضوع حماية أنظمة المعلومات بكل أشكالها المادية و اللامادية وأيضا مكونات أمن المعلومات و احتمالات انتهاك أمنها و سلامتها .

[1]- سعيدي، سليمة . ***الهاكرز وأمن المعلومات*** . مذكرة ليسانس: علم المكتبات : قسنطينة، جامعة منتوري 2006:

[2]- غزال، عبد الرزاق . ***أمن المعلومات الالكترونية وحقوق المؤلف في ظل التشريع الجزائري*** . مذكرة ماجستير: علم المكتبات : قسنطينة، جامعة منتوري : 2002

[3]- صادق، دلال . حميد ناصر.***أمن المعلومات***.عمان :دار اليازوري العلمية، 2008

[4]- دباس الحميد، محمد؛ ابراهيم نينو، ماركو . ***حماية أنظمة المعلومات.*** عمان: دار الحامد للنشر و التوزيع،2007



الفصل الأول:
ماهية مواقع الويب وخصائصها

خطة الفصل الأول

تمهيد

1-1- ماهية المواقع

1-1-1-مفهوم المواقع.

1-1-2- أنواع المواقع

1-1-3 أهداف المواقع

1-1-4- أهمية مواقع الويب.

1-1-5- مميزات المواقع.

1-2- تصميم صفحات المواقع.

1-2-1-أدوات البرمجة.

1-2-2-برمجيات تصميم المواقع.

1-2-2-1- برمجية Microsoft Frontpage.

1-2-2-2-برمجية Home site

1-2-2-3- برمجية ..Web Publisher

1-3-لغات تصميم المواقع.

1-3-1- لغة النصوص الفائقة HTML

1-3-2-لغة الجافا JAVA

1-4- معايير تقييم المواقع

1-5- دور المواقع في خدمة الباحث و البحث العلمي

خلاصة

تمهيد:

لقد أدت تكنولوجيا المعلومات و الاتصالات إلى ظهور شبكات وقواعد المعلومات التي أصبحت تقدم أحدث المعلومات في ثوان،لذا فعلى كل مؤسسة عملية تصبوا إلى النجاح من خلال تقديم خدمات أفضل، أن تتبنى هذه التقنيات والتكنولوجيات بما فيها مواقع الويب وبالتالي توافد جمهور المستفيدين إليها وسعيهم وراء لاستفادة من خدماتها.

1-1- ماهية المواقع:

<u>1-1-1-مفهوم المواقع:</u> يمكن تعريف موقع الويب بأنه عبارة عن صفحة ويب واحدة أو أكثر يقوم بإعدادها شخص أو شركة تكون مسؤولة على محتوى المواقع الخاص بها.[1]

كما يعرف انه سلسلة أو مجموعة من وثائق الويب حول موضوع معني تكون مخزنة في خادم ويب. [2] فموقع الويب هو كل متكامل قائم على هيكلة معقدة تسمح بتنظيم مختلف الصفحات وتحدد المسلك الذي يتخذه المستعمل عن طريق الروابط النصية ،وبعبارة أخرى فإن الموقع ما هو إلا ملف معلوماتي مخزن في حاسوب و هو (خادم الويب) مرتبط بشبكة الانترنت بصفة دائمة [3]، فهو بذلك مجموعة الوثائق المكتوبة بلغة النصوص الفائقة التي يضعها شخص أو هيئة تحت تصرف الآخرين عبر شبكة الويب.

<u>1-1-2- أنواع المواقع:</u> تتكون مواقع الويب من عدة أنواع حيث يرتبط كل نوع من هذه الأخيرة بالهيئة أو الجهة المصممة له و المسؤولة عنه.

* المواقع الحكومية: وهي المواقع الخاصة بالجهات الحكومية سواء داخل الدولة أو خارجها من خلال، الملاحظات المستنتجة من بعض الدراسات تحصلنا على نتائج تفيد أن نسبة إستخدام المواقع الحكومية لا يتعدى 10% وذلك يرجع إلى طريقة عرض المعلومات أو لتميزها في أغلب الأحيان بالإحصائيات

* المواقع الرسمية: هي مجموعة المواقع التي تتبع هيئات ذات صبغة رسمية نذكر مثالا عنها الجمعيات المتخصصة مثل موقع جمعية المكتبات الأمريكية[4]

---

[1] -Voss,Andrés. ***<u>Dictionnaire de l'informatique et de l'anterret</u>*** 1999 paris: micro .application 1998,p.502

[2] -Kent, péter. ***<u>le world wide web</u>*** paris: samad SM,1995,p.187

[3] -Bouche, gille. ***<u>tout savoir sur enternet</u>***.paris : ARLEA, 1996,p.63/64

[4] -Voss, Avdrées.op cit.p.247.

* المواقع الإخبارية: هي مواقع تحمل في طياتها الاختبار و التحليلات المتجددة يوميا ،أي باستمرار كمواقع القنوات التلفزيونية و الإخبارية.

* المواقع الإرشادية: وهي مواقع لأدلة البحث على الشبكة العالمية مثل ما هو الشأن بالنسبة لموقع ياهو Yahoo portail و قوقل google orateur.....الخ .وتعد هذه المواقع بالنسبة للباحثين موضوع الدراسة مهمة في البحث عن المعلومات، المتاحة عبر النوافذ الشبكة العالمية.

* المواقع التعليمية: تكون تابعة للجهات و المؤسسات التعليمية من أجل التعريف بها ووصفها، أو لغاية الاستغلال في التعليم عن بعد عبر المواقع الافتراضية.

3-1-1 أهداف المواقع :

لمواقع الويب أهداف كثيرة تتجلى في بعض النقاط نذكر منها:

- جعل المستفيد يصل إلى المعلومات في وقت قصير، وذلك عبر كتابة العنوان الالكتروني للموقع الذي يحتاجه خاصة عن طريق محركات البحث.
- تجنب الجهد الكبير وتضييع الوقت أثناء عملية البحث و هذا خاصة إذا كانت عملية الاستقبال عن طريق الأقمار الصناعية .
- إتاحة معلومات فورية وتنصف فورية للجمهور، وهذا يتم عن طريق النصوص الفائقة.
- إمكانية الوصول إلى البريد الالكتروني والاستفادة من خدمات أخرى[1]
- الاستفادة من خدمة الخط المباشر، وذلك بإتاحة الكثير من الخدمات للمستخدم التي هي مفيدة جدا له وتسهل له الحياة.
- مسايرة التطور التكنولوجي ومواكبة العصر من خلال مختلف المعلومات المعينة التي يقدمها.
- التعريف بمنتجات مختلف الشركات عن طريق وضعها في مواقع الويب خاصة بها، كما تستطيع الإشهار لمنتجاتها في مواقع أخرى.
- العمل على تسويق المعلومات من أجل استقطاب أكبر عدد من المستفيدين.

[1]- دايسون بيتر. ***ألفباء الانترنت***. لبنان: دار العربية : 1988، ص 98.

1-1-4- أهمية مواقع الويب:

تعتبر عملية إنشاء المواقع الالكترونية عملية منظمة ومهيكلة تتطلب مجهودات مكلفة، وهذا بغية الحصول على مواقع للمستفيدين تلبي لهم احتياجاتهم وطلباتهم، وتتجلى أهمية المواقع في البنود التالية:

- ➢ تقديم خدمات معلوماتية لا حصر لها في مختلف التخصصات و المجالات التي تهم المستفيدين.
- ➢ تقديم كم من المعلومات المحينة و الفورية.
- ➢ السرعة في الحصول على المعلومات في أقصر وقت ممكن خلافا عن وسائل البحث التقليدية[1].
- ➢ استقطابها لعدد كبير من المستفيدين كونها تصل إلى حشد أكبر عدد منهم .

1-1-5- مميزات المواقع:

لكي ننشئ موقعا ناجحا نتيح من خلاله المعلومات للباحثين على اختلاف تخصصاتهم لا بد أن يتوفر على المميزات التالية:

* الوضوح: بمعني أن يكون الموقع واضحا ومنظما وفي عدة صفحات فالأولى منها تعطي نظرة عامة على محتوى الموقع وهاما يجعله مهيأ، والثانية تمثل متن الموقع .

* سهولة الإبحار: وبالتالي تتيح لنا إمكانية الانتقال بسهولة من صفحة لأخرى،حيث تقوم بهذه العملية الصفحة المصنفة التي توجه الباحث إلى مكان تواجد المعلومات المتعلقة بموضوع بحثه.

*السرعة:تعتبر من أهم العناصر التي تساهم في نجاح استخدام أي موقع، وانعدام هذا العنصر يشكل عائقاً أمام عملية إتاحة المعلومات فمن الأفضل اجتناب الصور و الرسوم البيانية المتداخلة.

*أهمية وأصل المحتوى: قبل عملية إنشاء موقع ويب يجب التأكد من أصل وصحة المعلومات المراد بثها ، ومن ثمة العمل على إضافة معلومات قد يجعل الباحث أكثر استخداما للمعلومات لاسيما إذا كانت معروضة بطريقة جيدة باستخدام التكنولوجيا الحديثة للوسائط المتعددة.

[1]- شاهين،بهاء. ***شبكة الانترنت*** :مصر : كبيوسينس، 1996 ص 59

1-2- تصميم صفحات المواقع:

حتى يتمكن أي باحث من إنشاء صفحة أو موقع ويب لا بد عليه من الإلمام بمداخل ومخارج لغة « HTML » إضافة إلى وجوب توافر أربع أدوات رئيسية: برنامج تحرير النصوص لكتابة وتعديل ملفات HTML، ومعرفة جيدة بلغة HTML وبتقنيات الشبكة العنكبوتية ، مجموعة من الصور التي يحتمل أن يستخدمها في الصفحة ، برنامج بياني يتيح تحرير النصوص.

1-2-1-أدوات البرمجة : لإعداد صفحات المواقع ونشرها على شبكة الانترنت نحتاج إلى توافر مجموعة من أدوات البرمجة التالية:

***محرر النصوص:** يستخدم في كتابة برنامج تصميم الصفحات ، يتميز بالقدرة على حفظ الملفات بلغة الأسكي «ASCII» وبذلك يمكن من استخدام برنامج مثل Edition في بيئة Dos.[1]

***برنامج الرسم:** وهو عبارة عن برنامج يقوم بتحويل أشكال النصوص إلى صيغ لمبادلة الصور أو توضعها GIF: Graphique iInterchange Format

***برنامج التصفح :** يستخدم في الترجمة و اختيار النصوص التي يكتبها بلغة "Html" ثم ترجمتها إلى اللغة الطبيعية ، ويقدم هذا البرنامج النصوص و الصور و الأصوات و لقطات الفيديو كصفحة على الشاشة.

***جهاز خدمة الشبكة العنكبوتية:** تقع عليه مسؤولية نشر الصفحات المرجعية على الانترنت و ذلك بالاتفاق مع مزود الخدمة Provider الذي يقوم بخدمة الاتصال بالانترنت، بحيث يوفر الحاجة اللازمة لعرض المادة على الجهاز الرئيسي المتصل بالانترنت.[2]

1-2-2-برمجيات تصميم المواقع :

لقد قمنا باختيار ثلاث برمجيات وقمنا بتغطية بعض سيماتها المميزة مثل جعل الملفات متاحة للآخرين ليتمكنوا من تحميلها download

1-2-2-1- برمجية Microsoft Frontpage:

إن فرونتبايج منتج مميز يهدف إلى الجمع بين سهولة استخدام التطبيقات المكتبة الأساسية office دون أن يتعرض للمواصفات بسوء، تكمن الفائدة في الطريقة

---

[1]- شاهين ، بهاء.***المرجع العلمي لاستخدام الانترنت***.القاهرة : دار العلوم العربية،1997،ص.99.

[2]- رحابي ، توفيق؛ سلطاني،عبد المجيد.***الانترنت و إتاحة المعلومات داخل المحيط العلمي***:دراسة ميدانية بجامعة منتوري: ليسانس: علم المكتبات: قسنطينة،2000،ص.97.

الديناميكية التي يتبعها فرونتبايج في أنه يستطيع أن يستغل قدرة خدمات الويب لتنفيذ البرامج بدلا من مجرد استعمال ملفات .

كما يعد فرونتبيج برنامج لتحرير مستندات المواقع اعتمادا على لغة ترميز النصوص التشعبية html، ويقوم تلقائيا بإعداد الصفحات المرجعية و تحويل محتوياتها من نصوص وصور رسوم...إلى صفحات مكتوبة بلغة html.

1-2-2-2-برمجية Home site:

إن منشئ Home site هو حركة التحرير المباشر HyperText markup language وهي برمجية مميزة تعتمد على تحرير الترميز ,وتتوفر على واجهة تخاطبية مبهجة ومساحة تحريرها تتقبل عدة وثائق كما تتضمن علامتين في الأعلى؛ خصصت الأولى منها للترميز والثانية لمعاينة الصفحة.

وتستطيع هذه البرمجية استخدام متصفح Internet explorer في نافذة المعاينة،وذلك في حالة تنصيبه مسبقاً ، يقوم المحرر بإظهار الترميز بالألوان مع إمكانية إظهارها على كامل الشاشة.

1-2-2-3- برمجية Web Publisher[1]:

تتضمن معظم التطبيقات مرشدات إلا أن" WP" مرشد دون تطبيق يتم فيه إنشاء صفحات الويب وفق إجرائية خطوة بخطوة من خلال مربع حوار، نختار في البداية الموضوع ثم تصنيف الصفحات المعتمدة على واحد من أربع طرازات توضح أو تجمع كل واحدة منها عنوانا و رسما واحداً،فتظهر بذلك صورة مصغرة عن صفحة الويب المصممة وبالنقر المزدوج على النص في هذه الصورة ، يتم فتح محرر النصوص فيمكن إضافة نص ثاني، وبرمجية " WP" سهلة الاستعمال و صفحاتها مبهجة و لافتة للنظر.

1-3-لغات تصميم المواقع:

<u>1-3-1- لغة النصوص الفائقة HTML:</u>

هي اللغة التي تمكن من خلق الروابط النصية ، وهي لغة تستعمل لوضع صفحات الويب على الانترنت ، وهي تحتوي على سلسلة من رموز لغة « American Standard Code Fore Information Interchange » لكتابة النصوص ، كما تحتوي أيضا على تعليمات خاصة للروابط النصية التي تسمح بخلق الروابط بين عدة مواقع في الوثيقة نفسها أو بين وثائق أخرى متباعدة فيما بينها، تحتوي لغة النص المرجعي

---

[1]- بليرون ،نادية. *<u>تصميم مواقع البحث دعامة للشبكة الأكاديمية البحثية</u>*، ليسانس:علم المكتبات: قسنطينة.2003،ص.49.

Html على أوامر أو علامات تسمح بوضع وصلات مرجعية في أي وثيقة، بالإضافة إلى علامات تصف الوثيقة ،ويمكن ربط أي صفحة مرجعية بأي نوع من أنواع الملفات ، وفيما يلي بعض الوثائق التي يمكن ربطها بأي صفحة مرجعية: -الصفحات المرجعية المختلفة –ملفات الصور –مواقع نقل الملفات – الملفات الصوتية – عناوين البريد الالكتروني –مواقع الجوفر[1]

1-3-2-لغة الجافا JAVA :

لغة java كانت من أبرز الإضافات على عالم الانترنت في السنوات الأخيرة لأنها زودت المستخدمين بقدرة إنشاء الرسوم ، الموسيقى، وصفحات حية للتعامل بين المزود و المستخدم، ويمكن للمبرمجين حالياً استخدام لغتي البرمجة Visuel Basic أو Java Scripts، ليربط برامج Java بتحكمات أخرى تابعة لـ Active X .لتتوفر لهذه البرامج خيارات إضافية أكثر ليونة وذات نطاق أوسع، ولغة الجافا هي لغة برمجة تساعد متصفحات الويب على أن تضم برامج مصغرة تسمى بريمجات تظهر على شكل صور متحركة أو أصوات أو نصوص متتالية ولغة الجافا لديها عدة خصائص نذكر منها:

- إضافة الحركة و الصوت على صفحات الويب.
- كتابة الألعاب و البرامج المساعدة.
- إنشاء برامج ذات واجهة مستخدم رسومية.
- تصميم برمجيات تستفيد من كل مميزات الانترنت.

توفر لغة الجافا بيئة تفاعلية عبر شبكة الانترنت و بالتالي تستعمل لكتابة برامج تعليمية للتعليم الالكتروني و التعلم عن بعد.[2]

1-4- معايير تقييم المواقع:

بالرغم من النجاح الذي عرفته شبكة الانترنت و الانتشار الواسع و السريع الذي حققته في وقت قصير (قياسي)، و اعتمادها كأداة للتعامل في مختلف المجالات العلمية و الاقتصادية و الاجتماعية و الرياضية...الخ،إلا أنه توجد معوقات و مشاكل حالت دون سيرورة هذا النمو وحدت منه، أهم هذه المشاكل ما يتعلق بقيمة المعلومات المتوفرة على الشبكة، مما طرح قضية مصداقية و موثوقية و دقة هذه المعلومات.

---

[1]- شاهين،بهاء.المرجع نفسه،ص67.
[2]- الموسوعة العربية للكمبيوتر و الانترنت.الجافا سكريبت، [متاح على الخط]. http//www.geocities.com/teather.club.html تمت الزيارة يوم :2011/02/15.

يعود هذا المشكل أساسا إلى كون شبكة الانترنت تفتح المجال لأي منتج أو مؤلف مهما كانت درجته و مستواه العلميين، بان ينشر معلوماته عبر الشبكة العالمية دون أدنى قيد أو شرط و دون النظر إلى قيمة هذه المعلومات شكلا و مضمونا [1]، عكس ما هو عليه الحال في الوسط التقليدي و ما يمر عليه من عمليات المراجعة و التقييم و الانتقاء.

وعليه يمكن اعتبار تقييم مواقع الويب تلك العملية التي تهدف إلى تحديد قيمة الموقع من مختلف جوانبه المادية و الشكلية و الإعلامية ،باعتباره شكلا من أشكال مصادر المعلومات وفق طريقة منهجية معينة تتم من خلالها هذه العملية.[2]

-عنوان الموقع:

يحتل هذا الحيز عنوان الموقع المراد انتقاء المعلومات منه، وهو ما يعرف على الساحة التكنولوجية التقنية بـ" URL "، فهو العنوان الموحد لمواقع الويب الموجود ضمن خادم الويب على الانترنت، هذا الأخير يستعمل للوصول إلى المصادر الالكترونية المخزنة في الشبكة العالمية.

- سهولة الوصول إلى الموقع:

إن سهولة الوصول إلى الموقع في وقت سريع عامل أساسي لاستعماله و العودة إليه حيث أن هناك الكثير من المواقع التي يجد المستعملون صعوبة في الوصول إليها بسبب صعوبة تنزيل الصفحات الغنية بالصوت و الصورة، وهو ما نصح به مؤلفي و منتجي المواقع أي إلى ضرورة التقليص منها ورصها لتسهيل تنزيلها.

- مجال الموقع:

يبرز هذا العنصر في الصفحة الأولى للموقع ومن خلال الأقسام المختلفة التي يتضمنها، ويمكن الانتقال إليها عن طريق الضغط عليها باعتبارها روابط نصية تحيل إلى مصادر و صفحات أخرى داخل و خارج الموقع.

ويسمح الاطلاع على الموقع من خلال صفحته الأولى بتحديد مدى شمولية التغطية مثل ما يسمح به فهرس الكتاب،كما أنه يساعد في رسم حدود الموقع بحيث تعتبر الأقسام الظاهرة فيه جزءاً لا يتجزأ من الموقع نفسه.

-حداثة المعلومات:

---

[1]- مود اصطفان، هاشم. ***منهجية ومقاييس تقييم المواقع على الشبكة العنكبوتية: الإستراتيجية الموحدة للمعلومات في عصر الانترنت ودراستها***. 1998، ص.444

[2] -Kent.peter. le word wide web ، Paris: sand S.M 1995 p96

لابد من معرفة مدى حداثة المعلومات المحتواة في الموقع، من خلال معرفة تاريخ إنشاء الموقع، تاريخ آخر تحديث له، وكذلك من الضروري معرفة وتيرة التحديث، كما أنه لا تشكل حداثة المعلومات مقياسا جامدا إذ أن نسبتها تتغير مع طبيعة المعلومات فمثلا من غير الضروري أن يحدث الموقع المختص بالأدب اليوناني القديم بوتيرة عالية، مثلما هو الشأن للمواقع التي تعالج مواضيع علمية بحتة أو تقديم إحصائيات وأرقاما تتجدد باستمرار.

كما أن هناك معايير أخرى لا يمكن ذكرها جميعا منها : الجمهور و مضمون الموقع و كذلك معيار اللغة و التنظيم.[1]

1-5- دور المواقع في خدمة الباحث و البحث العلمي:

تعتبر مواقع الانترنت لمؤسسات المعلومات من أبرز ركائز التقدم الحضاري، كون هذه المؤسسات تتوفر على معلومات تمثل بدورها الركيزة الأساسية في الدراسات و البحوث العلمية ، فكل باحث هو بحاجة ماسة إلى قدر معين من المعلومات المتاحة على الخط التي تلعب دورا فعالا في تدعيم البحوث العلمية باعتبارها عاملا أساسيا لدفع عجلة التنمية إلى الأمام ، إذ تقوم بتزويد الباحث بكل المعطيات المفيدة و الضرورية لإنجاز بحثه العلمي كل حسب تخصصه.

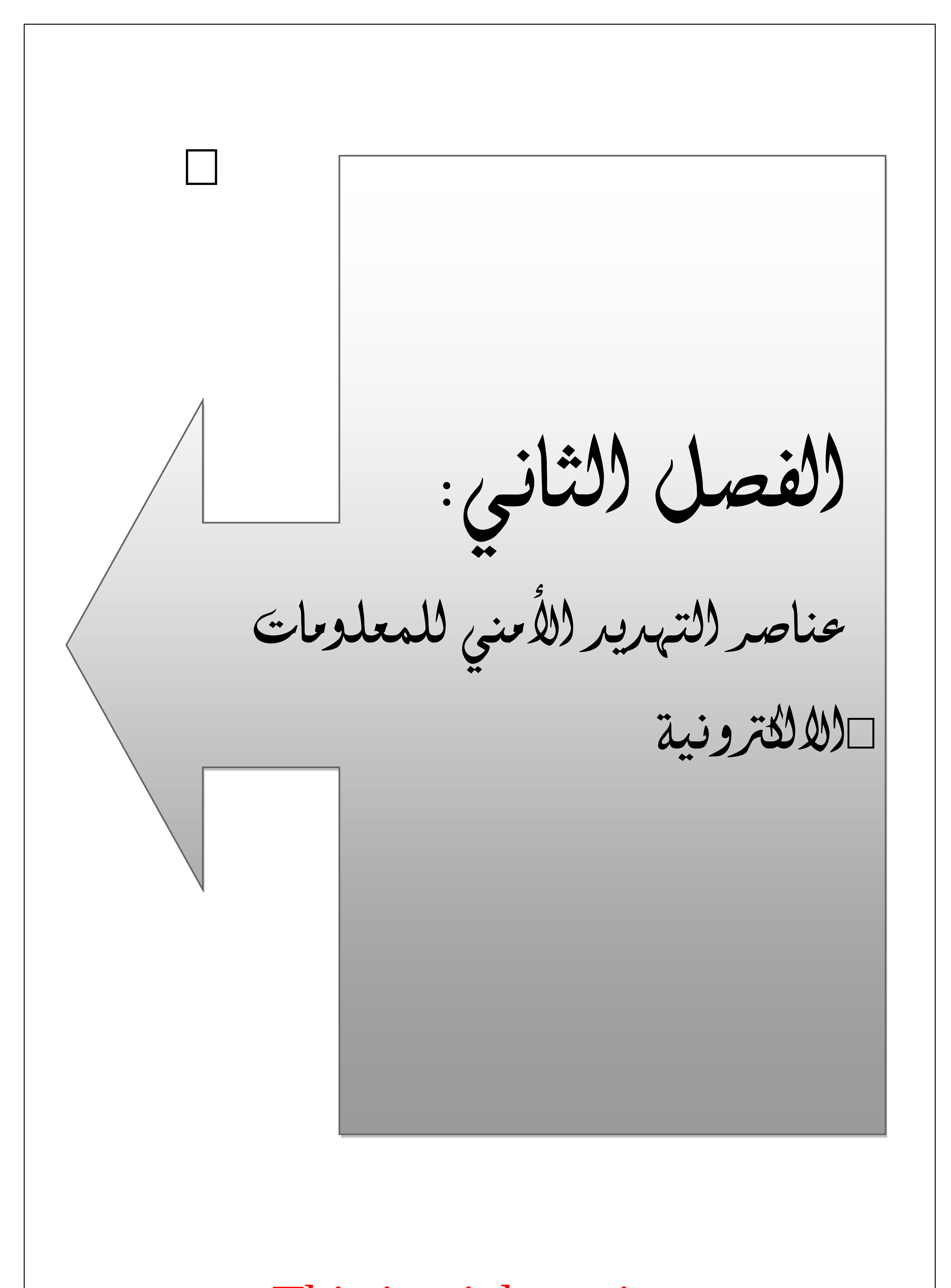
كما أن مواقع الانترنت تعد عنصرا أساسيا في أي نشاط بشري لما تتميز به من فعالية، فإذا كانت المكتبات وسيلة التقدم و الرقي فإن مواقع الويب تعد السند الأساسي لإنجاز أنفع البحوث العلمية و أجودها ، فمعلومات المواقع تعد الممون الرئيسي للباحث في إنجازه لمختلف المشاريع العلمية . وبذلك تبرز أهميتها في خدمة الأبحاث ،ولهذا وجب علينا القيام بجملة من التعديلات اللازمة و الخاصة لتطوير البحث العلمي و تنميته وهو الأسلوب التكنولوجي الذي يسهل عملية تقليص الجهد البشري و كذلك توفير الوقت و السرعة في الإنجاز لمواكبة الانفجار المعلوماتي المذهل الذي يتطور يوماً بعد يوم.[2]

[1]- غانم، نذير. *__تقييم مواقع الويب الجزائرية على الانترنت__*. ماجستير: علم المكتبات :قسنطينة،2002،ص.97
[2]- بليرون ،نادية. المرجع السابق، ص .90

خلاصة :

لقد أصبح دور مواقع الويب فعالاً ومتنامياً مساهماً في الحركة التنموية الشاملة لاسيما ونحن في عصر إقتصاد الخدمات الذي يعتمد بالدرجة الأولى على المعلومات .

إن الارتقاء بالمستوى الثقافي و المعرفي الجامعي أصبح من أصعب المهام الملقاة على عاتق الجامعات و خصوصاً ونحن بأمس الحاجة إلى جيل يملك ثقافة المعلومات، يضع نصب عينيه المعرفة العلمية و الأسلوب العلمي في التفكير و التحليل و التقويم خدمة لأهداف مجتمعه.


الفصل الثاني:
عناصر التهديد الأمني للمعلومات
الالكترونية

خطة الفصل الثاني

تمهيد

2-1- تعريف التهديدات الأمنية

2-2 أنواع التهديدات الأمنية.

2-3- أسباب التهديدات الأمنية.

2-4 المجرم المعلوماتي.

2-4-1 الهاكرز.

2-4-2 الكراكرز.

2-4-3- الفرق بين الهاكرز و الكراكرز.

2-5 الفيروسات.

2-5-1- أنواع الفيروسات.

2-5-2 أشهر الهجمات الفيروسية(نماذج من فيروسات المعلومات) .

2-5-3- الديدان الفيروسية.

2-5-4- برامج ذاتية التحميل وأحصنة طروادة.

2-5-4-1-برامج ذاتية التحميل.

2-5-4-2- أحصنة طروادة(trojan horses) .

2-6- كيفية الاختراق.

2-7-عملية تشويه موقع ويب.

خلاصة

تمهيد :

إن الارتباط بشبكة الإنترنت يعطي مجموعة سريعة من عناصر المعلومات للمستعمل وكما أن هناك استعمال موجب لعناصر الانترنت ، يوجد جانب مظلم حيث يسيء بعض الناس استعمالها باعتبارها بحر مفتوح من عمليات الكمبيوتر فهي معرضة أكثر من غيرها للكثير من المخاطر التي تهدد أمن التجهيزات و المعلومات معاً.

2-1- تعريف التهديدات الأمنية:

لا يوجد تعريف موحد للدلالة على التهديدات الالكترونية, فتعددت التعاريف واختلفت باختلاف وجهات النظر ,ويمكن لنا عرض أهم التعاريف التي تناولتها الدراسات الدولية, فيعرفها مكتب المحاسبة بالولايات المتحدة الأمريكية بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه " وتعرف بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات " أو هي " أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات " أو هي " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر"

ويعرفها تاديمان بأنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب "وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا "

ونحن نرى أن أرجح التعاريف هو تعريف منظمة التعاون الاقتصادي والتنمية,وهو" كل فعل أو امتناع من شانه الاعتداء علي الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات فيتسم هذا التعريف بالوضوح هذا فضلا عن تحديده لماهية السلوك الإجرامي للجريمة التي قد تقع به إذ شمل كلا من الفعل الايجابي والسلوك السلبي المتمثل في الامتناع".[1]

1- صابر، دويب حسين. ***المؤتمر السادس لجمعية المكتبات و المعلومات***. السعودية: الرياض، 2008.

2-2 أنواع التهديدات الأمنية:

❖ **تهديدات التجهيزات :** تعتبر التجهيزات المكون الأول في نظام المعلومات و تتعرض إلى المخاطر التالية:

- سرقة التجهيزات كسرقة أجهزة الحواسيب أو أحد أطرافه سواء كانت مادية أو معنوية.
- تعطيل أحدى هذه التجهيزات، وذلك عن طريق العبث بها من قبل أي شخص .
- تدمير هذه الموارد بالنار كأن يكون الحريق متعمدا أو عن طريق المياه أو عن طريق الطاقة الكهربائية.
- عمل نسخ عن مفاتيح الدخول للنظم و المواقع [1]

❖ **تهديدات البرمجيات:** تعتبر المكون الثاني في نظام المعلومات وتتعرض إلى المخاطر التالية:

- الدخول غير المشروع إلى موقع الحواسيب والشبكات وتعديل أمور فيها .

- تخريب البرمجيات وتشويشها غما نتيجة عطل أو باستعمال برمجيات خبيثة مثل: الفيروسات حصان طروادة الأبواب الحلقية...الخ.

❖ **تهديدات المعلومات** : تعتبر المعلومات المكون الثالث في نظام المعلومات وتتعرض إلى:

- حذف الملفات التشويه الناتج عن مشاكل في الأجهزة أومن علة في البرامج إضافة إلى كافة الاختراقات و القرصنة[2]

1- العامري، محمد فاروق. ***الانترنت***: القاهرة : دار الفكر العربي، 1997. ص.ص.115-114.

2- حسين، عبد الله، محمود، علي. ***سرقة المعلومات المخزنة في الحاسب الآلي***. القاهرة: دار النهضة،2001،ص.116.

2-3- أسباب التهديدات الأمنية:

إن التزويد و التلاعب بالأنظمة المنفذة على الحاسب هو من نفس الطراز الذي يتم في مراحل الأنظمة اليدوية لكن استخدام الحاسوب بهذا الشكل الواسع أفرز وسائل جديدة في ارتكاب دائم للتزوير و التلاعب بالأنظمة و تدميرها و قد ساعد في ذلك :

- **الفرص المتزايدة:**

إن ازدياد مستخدمي الحاسوب من ذوي المقدرة و المعرفة على الاختراق نتيجة لامركزية معالجة شبكات الاتصالات و الدخول عن بعد إلى الحاسوب قد استخدمت فرصا متناسبة ومتزايدة للمزورين و المتلاعبين لتنفيذ أغراضهم خاصة في ظل سيطرة رقابة غير كفأة في هذا المحيط الالكتروني

- **صعوبات الاكتشاف:**

إن وجود كميات كبيرة من المعلومات المخزنة في الحاسب يجعل إخفاء أو تزوير أو أي تلاعب عملية سهلة، خاصة إذ تمكن مرتكب الجريمة من عدم ترك أي دليل خلفه، الأمر الذي يترتب عنه صعوبة اكتشاف الجريمة.

- **تحقيق الأرباح:**

نتيجة للأرباح الطائلة التي يمكن أن يجنيها مرتكب الجريمة "تزوير أو تلاعب أو إخفاء..." فإنها تشكل واقعا قويا لأصحاب النوايا السيئة في ارتكاب جرائمهم ، وقد قدر باحث أمريكي الأرباح التي يجنيها مرتكبي الجرائم الالكترونية 600ألف دولار - مقابل 300 ألف لمرتكبي الجريمة في النظام اليدوي[1]

2-4 المجرم المعلوماتي:

المجرم المعلوماتي هو ذاك الشخص أو مجموعة من الأشخاص التي تتخذ من عملية السطو أهدافا لها وينقسم المجرم المعلوماتي إلى:

2-4-1 الهاكرز: ويحمل معنى المتخصص في نظم المعلومات و البرمجيات وهي عبارة عن اسم اختاره لأنفسهم مجموعة من المبرمجين أكفاء المهرة القادرين على ابتكار البرامج وعلى حل مشكلات البرامج في الحاسب الآلي وفي جميع الأنظمة و التعامل مع الشبكات وأول هاكرز هو "تيورفالدس ليونكس" أحد أهم

1- صادق، دلال؛ الفتال، حميد ناصر. ***أمن المعلومات.*** عمان: دار اليازوري العلمية، 2008، ص.45.

مطوري نظام التشغيل Unix وهو أيضا مبتكر النظام الأكثر أمانا وشهرة في العالم Linux .

ويعد الهاكرز أو القرصان المحترف مبرمج ذي مهارة عالية يسعى لاكتشاف الثغرات و نقاط الضعف في نظم الحماية الخاصة بأنظمة التشغيل ،ويكتفي الهاكرز بعمليات الاختراق دون العبث بالملفات على عكس النقيض في رأيهم مجرمين ومدمرين يجب معاقبتهم .[1]

2-4-2 الكراكرز: هو شخص خبيث متطفل وفضولي يسعى إلى اكتشاف الحقائق و الأخبار من خلال التطفل بالوسائل الغير قانونية وهم فضلا عن ذلك أشخاص عاديون يشغلون مناصب محا ثقة ولديهم الكفاءة الخاصة و المعرفة و المهارة المطلوبة في مجال الكمبيوتر.

ويعرف كذلك على أنه الشخص الذي يعمل عل ى فك أكواد البرامج التي يحصل عليها أو اختراق وتعديل هذه البرامج بالاعتماد على الثغرات و الهفوات داخل الأنظمة، كما يسعى إلى اختراق أنظمة المعلومات بالبحث عن كلمات المرور.

2-4-3- الفرق بين الهاكرز و الكراكرز:

إن الكتابات المعاصرة جعلت كلا من مصطلحي الهاكرز و الكراكرز وجهين لعملة واحدة وهي الدمار و الخراب داخل الأنظمة ويمكن الفرق بينها فيما يلي:

أ **-أوجه التشابه :** صرح بعض خبراء مكافحة جرائم الكمبيوتر إن أفضل وسيلة للتعرف على الأشخاص ذوي الميول الإجرامية هي تحليل وتقييم مهاراتهم و معارفهم وخبراتهم الفريدة و غالبا ما يكون مرتكب الجريمة الإلكترونية قوي الذاكرة وذو ثقافة راقية و من الغريب إن هذه الخصائص تؤهل هؤلاء الأفراد لشغل وظائف مرموقة في ميادين الكمبيوتر المختلفة وفي الكثير من الأحيان تبدو شخصياتهم محبوبة لدى الناس من دون معرفة أنهم من الهاكرز و الكراكرز لكنهم يحبذون الانعزالية و الاختلاء بأنفسهم معظم الوقت . وقد تكزن عبقريتهم هي سبب شعبيتهم الجارفة من يدري؟قال مرة مسؤول كبير بأنهم"روبن هود الانترنت".

ب **-أوجه الاختلاف:** أصبح مصطلح الهاكرز يصف من يلجون إلى أنظمة شبكة المعلومات دون أن يفسدوا فيها و إنما يدفعهم الفضول و الرغبة في المغامرة وعليه تعلم المزيد عن تقنية معينة أو محاولة قهر النظام ، بينما الكراكرز على العكس النقيض ومن ذلك فهي كلمة تحمل كل معاني التخريب و الكسر و العبث و

---

[1] شوقي،حسام.***حماية وأمن المعلومات على الانترنت***.القاهرة:دار الكتب العلمية،2003،ص.95.

التحطيم حيث أن الكراكرز هو شخص يتسلل و يقوم باختراق شبكات المعلومات دون تصريح ويكون الهدف من الدخول هدفا شريرا و نوايا خبيثة إما لإتلاف الملفات – سرقة البيانات وذلك لغرض الربح أو الانتقام[1]

2-5 الفيروسات:

هي عبارة عن برنامج يتكون من مجموعة تعليمات مكتوبة بلغة راقية أو غير راقية يحدث بعد تنفيذه تغييرات وظيفية تجعل النظام المعلوماتي معاقا ولا يعمل بطريقة اعتيادية و صحيحة.[2]

وفي تعريف آخر : فالفيروسات عبارة عن برامج صغيرة تستغل البريد الإلكتروني سبيلا لتسللها إلى أجهزة الحاسوب ويعتبر البريد الإلكتروني من أكثر الوسائل شيعا لتسللها حيث يأتي في شكل ملف صغير ملحق بوسائل إلكترونية عندما يحاول المستعمل فتح الملف المرفق يشتغل البرنامج الكامن فيه و يصيب محتويات الحاسوب بأضرار كبيرة.[3]

2-5-1- أنواع الفيروسات : للفيروسات أنواع كثيرة و متعددة و في كل يوم تستحدث أنواع جديدة و لكن في مجملها يمكن حصرها في الأنواع التالية:

*فيروسات برامج التحميل (virus de secteure de boot) : تعتبر من أقدم الفيروسات المعروفة لدى المستخدمين حيث تستطيع أن تصيب القرص الصلب و الأقراص اللينة و تكمن خطورتها في قدرتها على إصابة جزء أساسي من أي صلب أو لين و هو الجزء المخصص لتوجيه الجهاز في كيفية تحميل نظام التشغيل ويقوم هذا النوع بتحميل نفسه للذاكرة في كل مرة يتم تشغيل الجهاز فيها.

* فيروسات البرامج (virus de programme): هذه الفيروسات مقيمة في الذاكرة و هي تصيب ملفات القابلة للتنفيذ ففي حالة تنفيذ هذه الملفات يشتغل الفيروس وهذه الفيروسات تحتوي على إحدى علامات الامتداد التالية: .sys.com

---

[1] - الزغيبي ، فهد بن عبد الله. ***الحماية و الهاكرز في عيوب البشر.*** [متاح على الخط]. تمت الزيارة يوم2011/01/11، متواجد على الرابط www.jazirah.com.sa/services

[2] - عبد الحق، طه . ***مدخل إلى المعلوماتية:العتاد و البرمجيات.***الجزائر : قصر الكتاب .2000،ص.218.

[3] - شيب، نبيل.***فيروسات*** http://forum.kuwaitup.com/t379315.html - تمت الزيارة يوم2010/12/25 ***الديوان***،.متاح على الخط

*الفيروسات الشكلية(poly morphes) : هي فيروسات متعددة الأشكال تحتوي على مفتاح تشفير يتغير محتواه بعد كل إصابة و للبعض منها مجموعة هامة من التوفيقات.

*الفيروسات الخفية (virus furitifs): هي حديثة و متطورة ,لها القدرة على التخفي بحيث لا يمكن للنظام المعلوماتي أن يتنبأ بوجودها و البعض منها لا يغير من حجم الضحية و البعض الأخر يزيل إصابة الملفات لحظة استدعائها من طرف النظام، ويعيد إصابتها بعد زوال الخطر[1].

2-5-2 أشهر الهجمات الفيروسية(نماذج من فيروسات المعلومات):

من أشهر الفيروسات التي انتشرت بطريقة وبائية و بسرعة فائقة لتصيب الملايين من الأجهزة حول العالم هي ما يلي:

- فيروس ميلسا Melissa virus:هي من أسرع الفيروسات التي انتشرت عام1999 و هي من نوع –ماكرو-تقوم بالانتشار عن طريق فيروس متخصص في إصابة البريد الالكتروني و الالتصاق في برامج النصوص كملحق في رسالة الكترونية[2].
- فيروس explore zip: وهو فيروس مشابه للسابق ،ولكنه مدمر أكثر ،يقوم بمسح كل الملفات التي أنشأت بواسطة برنامج تحرير النصوص.
- فيروس cih virus:وهو من أخطر الفيروسات ،لأنه قادر على مسح القرص الصلب و إصابة البرنامج الأساسي المسؤول عن المخرجات و المدخلات للجهاز ،مما يسبب تلف اللوحة الأم.
- فيروس الحب love virus :هو مشابه لفيروس ميلسا ، ولكنه متخصص في إصابة برنامج مايكروسوفت microsofte و البريد الالكتروني، وتسبب في تعطيل ملايين الملفات الالكترونية ، وورد هذا الفيروس في نسختين "نكتة جون" و "أنباء مضحكة أو فاني نيوز".وقد أصاب هذا النوع من الفيروسات حوالي 13 مليون حاسب في العالم[3].

[1]- عبد الحق، طه .المرجع السابق.ص.219.
[2]- فيروسات الانترنت[متاح على الخط].www.safola.com/antiverus.chtml تمت الزيارة يوم: 2011/02/02.
[3]- فيروسات الانترنت. [متاح على الخط]. المرجع نفسه.

2-5-3- الديدان الفيروسية:

هي نوع مبرمج بحيث لا تحتاج إلى تشغيل من جانب صاحب الحاسوب بإجراء ما ، كفتح الملف المرفق برسالة الكترونية مثلا، ويمكن الفيروس الدخيل من الاختفاء فترة من الوقت ثم يشتغل تلقائيا بعد ذلك في الموعد المحدد له من جانب مبرمجه ، فيفعل فعلته على غير انتظار من صاحب الحاسوب.

وأول ما ظهر هذا النوع من فيروسات الديدان عام 1988 ، وقد تسلل إلى خزانات الشبكة التي عرفت وقتها باسم arpanet التي كان ظهورها مقدمة لانتشار الشبكة العنكبوتية العالمية ، وقد وصل إلى سائر أجهزة الحواسيب المرتبطة بها وكان حينها يرتبط بهذه الشبكة حوالي 60 ألف مركز لتخزين المعلومات ، واحدث دمارا كبيرا في تسجيلاتها و محتوياتها ولم يستطع أحد منعه من ذلك.

مبرمج هذه الدودة الفيروسية هو شاب في الـ 23من عمره ،ابن المسؤول عن تأمينات الحاسوب في وكالة أمن الدولة وهي أكبر أجهزة المخابرات في الو.م.أ.[1]

***أشهر هجمات فيروسات الديدان(نماذج من الديدان الفيروسية):**

- ✓ دودة نيمدا(win32/nimda.a.worm): تعتبر من أشهر وأخطر الديدان الفيروسية وكلمة -نيمدا- تأتي من الكتابة العكسية لكلمة "أدمين- .Admin "وتعني مدير الشبكة ، فهي تصيب أجهزة الكمبيوتر وتتسبب في إلحاق الخراب على شبكة الانترنت[2]
- ✓ دودة كودريد(cod red):أو ما يسمى بالرمز الأحمر، هذا الفيروس من فيروسات الديدان الكمبيوترية وهي متميزة إذ أنها تتحرك بنفسها وتنسخ نفسها ، عكس الفيروسات الأخرى التي تتحرك نحو نظم الكمبيوتر بواسطة ملف أصابته.وكلمة كودريد اسم لأحد المشروبات الشعبية الغنية بمادة "الكافيين" التي يعشقها مبرمجو الكمبيوترات.

2-5-4- برامج ذاتية التحميل وأحصنة طروادة:

2-5-4-1-برامج ذاتية التحميل: تعتبر من بين البرامج التي تستعمل من قبل الأشخاص كأسلحة فتاكة للهجوم على الأجهزة وشبكات الانترنت و التجسس على

1- شيب ، نبيل. المرجع نفسه. تمت الزيارة بتاريخ2011/02/02

2- فيروسات نيمدا. [متاح على الخط]. http://www.alsaher.net/mjales/t4736.html تمت الزيارة يوم2011/02/05

المعلومات، وفي حالة وصولها إلى أي جهاز كمبيوتر فإنها تسمح بالتحكم الكلي و التام فيه عن بعد.

وللبرامج ذاتية التحميل ثلاثة أنواع وهي:

- برنامج أكتيف اكس (Active x) :وهي عبارة عن مجموعة من المتحكمات المبرمجة بواسطة برنامج مايكروسوفت، وصممت أساسا بعض التقنيات المستخدمة لإنشاء الصفحات المتطورة جداً، كما تمكن مصممي الصفحات من إنشاء صفحات بها الكثير من الحركات و الخصائص الجذابة، أما مخاطرها فتتمثل في:

-التحكم في نظام التشغيل بجهاز الضحية والتحكم في القرص الصلب ونقل الملفات من جهاز لآخر.

- برنامج جافا ابليتس :هي عبارة عن برامج صغيرة وشبيهة جداً بالأولى ، ولها نفس القدرات و هي خطيرة على أمن و خصوصية المستخدم.

- برنامج جافا سكريبت(Java script): يختلف هذا البرنامج عن سابقيه ،لكنه مشابه بالاسم فقط ، وهذا البرنامج باستطاعته فتح وغلق النوافذ أثناء العمل على الشبكة.وتكمن خطورته في قدرته على تعديل خصائص المتصفح الخاص.[1]

2-5-4-2- أحصنة طروادة(trojan horses): هو جزء من الكود ،يضاف إلى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات، ويؤدي عملاً تخريبيا للنظام ، وتكمن خطورته في أن النظام لا يشعر به وبوجوده حتى تحين اللحظة المحددة له ليؤدي عمله التخريبي.[2]

ولأحصنة طروادة صورتين ؛صورة انتقامية وصورة خفية،ومن المستحيل مراقبة وفحص هذه الأخيرة ، ولا توجد لحد الآن برامج تحدد البرامج المفيدة من الضارة ، وهدف أحصنة طروادة هو تهريب ملفات مدمرة إلى داخل الجهاز الخاص وهو هدف خفي وسري من خلاله يمكن جمع المعلومات ونقلها إلى جهة أخرى.

ولأحصنة طروادة عدة أنواع نذكر منها:

- **باك أورفيس (Back orfice):** هو أحد أنواع أحصنة طروادة الشهيرة، وقد تمت برمجته من قبل مجموعة يسمون أنفسهم (cult of the dead.com) وأساس

[1] - برامج ذاتية التحميل [متاح .www.safola.com/exc-programe.chtml>تمت الزيارة يوم 2011/01/05. على الخط] <

[2] - داوود،حسن الطاهر. ***الحاسب وأمن المعلومات***، الرياض:مكتبة الملك فهد الوطنية.2000 ،ص.ص.77.76.

فكرة البرنامج هو وضع خادم "باك أورفيس " في الجهاز الخاص، بحيث لا يعلم مستخدم الشبكة بوجوده عنده.

- **القنابل المنطقية:** هي أحد أنواع أحصنة طروادة ، وصممت لكي تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين ، وتؤدي إلى مسح بعض البيانات أو تعطيل النظام عن العمل.

- **القنابل الموقوتة:** القنبلة الموقوتة هي نوع خاص من القنابل المنطقية ، وهي تعمل في ساعة محددة وفي يوم محدد من طرف مصمم البرنامج.

- **باب المصيدة(trop door):** هذا الكود يوضع عمداً بحيث يتم لدى حدوث ظرف معين لتجاوز نظم الحماية والأمن في النظام ، ويتم زرعه عند تركيب النظام، وهو يظل كامناً غير مخرب حتى يقرر المخرب استخدامه. [1] وقد ظهر نوع آخر من أحصنة طروادة-تجمع من كل بحر قطرة- حيث أنها تستفيد من ميزة كل نوع من العناصر السابقة الذكر ودمجها مع بعض ،فمثلا يكون لها خاصية التكاثر مثل الفيروسات ولا تحتاج إلى برنامج يحتضنها مثل الديدان .ولديها القدرة على التعامل مع الملفات الصادرة والواردة من نوع ftp.[2]

2-6- كيفية الاختراق:

الاختراق بشكل عام هو القدرة على الوصول إلى هدف معين بطرق غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف ، كما يقصد بالاختراق قدرة المخترقين على الدخول إلى جهاز شخص معين بغض النظر عن الأضرار التي قد يحدثها.

وبعد أن تعرضنا إلى مفهوم الاختراق يعني أن نعرف كيف تتم هذه العملية !!!

تتم عملية الاختراق عبر عدة طرق ،أبسطها و التي يمكن للمستخدمين استخدامها و هي البرامج التي تعتمد نظام "الزبون الخادم "" "client /serveur حيث تحتوي على ملفين أحدهما serveur يرسل إلى الجهاز المصاب بطريقة ما والأخر الخادم يتم تشغيله من قبل المخترق للتحكم في الجهاز المصاب،وعند تشغيل ملف الـ serveurمن قبل المخترق يصبح الكمبيوتر عرضة للاختراق حيث يتم فتح أحد المنافذ

---

[1]- داوود،حسن الطاهر. المرجع نفسه، ص. 77

[2]- برنامج الأشرار وأسلحة الهاكرز.[متاح على الخط]< www.Safola.com/lolis.chtml تمت الزيارة يوم 2011/02/06

ports باستعمال برامج متخصصة في الاختراق كالـ back orfice net bus و يفعل ما يحلو له، فيما تستعمل طريقة جديدة للاختراق عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر الانترنت ،فيتم اعتراض تلك البيانات للتحكم في الجهاز الخاص.[1]

2-7-عملية تشويه موقع ويب:

يتبع المخترقون أساليب عدة في عمليات تشويه صفحات الويب و تختلف هذه الأساليب بناءا على نوع نظام التشغيل، ومزود الويب الذي يعتمد عليه الموقع ومن بين هذه الأساليب:

- **الدخول بهوية مخفية:** عبر منفذ بروتوكول ftp وتمكن هذه الطريقة المخترق من الحصول على ملف كلمة الدخول المشفرة الخاصة بأحد المشرفين على الشبكة، أو من يملكون حق التعديل على محتويات الموقع والعمل على فك تشفيرها. ويلجأ المخترقون بعد الحصول كلمة السر إلى استخدام برامج خاصة لتخمين كلمات السر كبرامج Force Crackers/Jack carakers brut ،وتعمل هذه الأخيرة على تجربة جميع الاحتمالات الممكنة لكلمة السر.
- **استغلال الثغرات الأمنية في مزودات الويب وأنظمة التشغيل:** لا يخلو أي نظام تشغيل أو مزود ويب من ثغرات أمنية تعرض مستخدمه لخطر الاختراق ، ويبقى المخترقون في استغلال الثغرات الأمنية حيث تبقى متاحة إلى غاية اكتشافها ،ويلجأ الهاكرز عند اكتشاف أي ثغرة أمنية إلى التستر عليها وعدم كشفها، ولا يعلنون عنها بسرعة حتى يتمكنوا من استغلالها لفترة أطول.[2]
- **استخدام بروتوكول TALENT :** تسمح الكثير من الثغرات الأمنية في الأنظمة المختلفة سواءً كانت بونكس أو ويندوز باستخدام تطبيقات تعتمد على بروتوكول TALENT الذي يسمح بالوصول إلى أجهزة الكمبيوتر عن بعد ، ويمكن استخدام هذا البروتوكول للدخول إلى مزودات الويب و تغيير الصفحات فيها.

[1] - سيدهم،خالد هناء.*المراسلات الالكترونية داخل محيط البحث العلمي*.جامعة منتوري قسنطينة:قسم علم المكتبات؛1999.ص.ص.80.79.

[2] - غزال،عبد الرزاق.عزيزي ،حكيم.*أمن المعلومات الالكترونية وحقوق المؤلف في ظل التشريع الجزائري*، جامعة قسنطينة:قسم علم المكتبات:2002. ص.97.

خلاصة:

كانت هذه أشكال وطرق القرصنة و الاختراق التي أصبحت من أحدث المشكلات التي تواجهها أنظمة الكمبيوتر بحيث أصبحت تهدد أمن المعلومات و الشركات و المواقع الحكومية ، وتسببت في إغلاق العديد من مواقع الانترنت، ويشير الخبراء إلى أن هناك صعوبة في مواجهة عمليات القرصنة ويرجع السبب إلى البرمجيات التجارية المعنية بمنع حصول القرصنة على اختلاف أشكالها و التي ما تزال في مرحلة التطوير.



الفصل الثالث:

أمن معلومات المواقع الالكترونية

خطة الفصل الثالث

تمهيد

3-1- تعريف أمن المعلومات

3-2- أهمية أمن المعلومات

3-3- أشكال الحماية الالكترونية

3-3-1- البرامج المضادة للفيروسات.

4-3-1-1- مفهومها

3-3-1-2- تشغيل البرامج المضادة للفيروسات

3-3-2- برامج جدران النار

3-3-3-ملقمات الانترنت

3-3-4- التشفير (Encryptions)

3-4 – برتوكولات أمن المعلومات

3-5- خطوات أمن المعلومات

3-6- دور الجامعات والمعاهد العلمية في تطوير آلية التعامل مع النظم المعلوماتية

خلاصة

تمهيد:

من السهل أن نبني قلعة مسلحة محكمة التحصينات ،لكن من الصعب أن نجعل الإقامة فيها سهلة وممكنة ومن هنا ننطلق لنعرض إشكالية جديدة لا تقل أهمية عن سابقتها ،وهي مشكلة الأمن ،والأمن الذي نقصد هنا هو أمن المعلومات الالكترونية المعروضة أو التي تدور عبر الشبكة العنكبوتية .

3-1- تعريف أمن المعلومات:

يقصد بالأمن تأمين وحماية كافة الموارد المعلوماتية المعروضة على شبكة الانترنت عن طريق إتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات .

كما يقصد به:القيام بمجموعة من الإجراءات أو الترتيبات الفعالة لحماية الجهاز أو الشبكة والمعلومات الخاصة والهامة وحماية الخصوصية .

وبالتالي فإن أمن المعلومات هو مجموعة الخطوات التي تهدف إلى حماية الحاسوب والمعلومات المخزنة داخله من الاختراقات والفيروسات وغيرها من عناصر التهديد الأمني للمعلومات من خلال مكافحة ملفات التجسس وحماية المعلومات الخاصة الشخصية.[1]

3-2- أهمية أمن المعلومات:

تكمن أهمية المعلومات في أنها تستخدم من قبل الجميع بلا استثناء، كما إنها هدف للاختراق من قبل الجميع وبلا استثناء أيضا......

وكثيرا ما تكون المعلومات هي الفيصل بين النصر والهزيمة في الحروب وأحيانا تكون الفيصل بين المكسب والخسارة لدى الشركات ،وقد انقلبت الآية في عصرنا هذا فلم تعد المشكلة في الحصول على المعلومات بقدر ما تكن في هذا السيل والفيض الهائل من المعلومات وكيف يتم التفريق بين الثمين منها والغث[2]

ومن ثم كيف يمكن حمايتها وتأمينها من جميع المخاطر ،لنخلص أن أهمية الأمن تتناسب طردياً مع أهمية المعلومات .

[1] أمن المعلومات. [متاح على خط]: *URL:safola.Com/security. chtml*. تمت الزيارة يوم:2011/02/10

[2]- داود ،حسن الطاهر. المرجع السابق ،ص. 11

3-3- أشكال الحماية الالكترونية:

3-3-1- البرامج المضادة للفيروسات :

4-3-1-1- مفهومها :

هي برامج تقوم بالحماية من هجمات الفيروسات وبقية البرامج التي تشكل تهديدا أمنيا على المعلومات ،وتستطيع أن تحدد الملفات الضارة القادمة من أي مصدر ،مثل الأقراص المدمجة اللينة والرسائل الالكترونية وكذلك يمكنها رصد هذه البرامج من القرص الصلب.

وتتكون البرامج المضادة للفيروسات من جزئين مختلفين:

- التشغيل المباشر عند الدخول: ويعمل هذا الجزء تلقائيا عند تشغيل البرامج أو تنزيل الملفات من الانترنت وهو ما يعرف بـ onaccesselement

- التشغيل عند الطلب: ويعمل هذا الجزء بناءا على طلب من المستعمل، وهو متخصص بالكشف عن أحصنة طروادة والفيروسات في القرص الصلب و الأقراص اللينة والمدمجة وهو ما يعرف بـ ondemondelement

3-3-1-2- تشغيل البرامج المضادة للفيروسات:

البرامج المضادة للفيروسات عبارة عن تقنية مسح ورصد للبرامج المشبوهة التي تتميز بخصائص معينة أو تحتوى على صيغة معينة من البرمجة، وهي عبارة عن مجموعة الأرقام الثنائية التي تعرف بالتوقيع ويتم ذلك بالطريقة التالية:

- يقوم البرنامج بالنظر إلى كل الملفات ذات الطبيعة التنفيذية ويتم مقارنة التوقيع الموجود على كل الملفات المخزنة في قاعدة المعلومات الخاصة بالبرامج المضادة للفيروسات.

نشير فقط أن كل برنامج مضاد للفيروسات يحتوى على أكثر من 4000 نوع من الفيروسات وأكثر من عشرة آلاف توقيع أحصنة طروادة والديدان .

كما يقوم بعد عملية المقارنة بإكتشاف الفيروس يقوم بإعلام المستخدم وبعد ذلك يقوم البرنامج المضاد بتخيير المستخدم بين مسح وتعطيل الفيروس أو إصلاح الخلل بطريقة آلية.[1]

---

[1]- غزال، عبد الرزاق .المرجع السابق ،ص. 49

3-3-2- برامج جدران النار:

المفهوم: هي أداة تصفي –تحجز- مرور البيانات والمعلومات داخل الشبكة أي بين الحاسوب الشخصي أو الشبكة الخارجية التي هي مصدر الخطر، وبالتالي تكمن أهمية أو مهمته في حجز كل ما هو غير مرغوب فيه خارج البيئة المحمية، وقد عملت برمجيات جدران النار مع عدة أنظمة،غير أنها في السنوات الأخيرة أصبح نظام مايكرو سوفت ويندوز، المنصة المستخدمة للعديد من الخدمات الشبكية وبرامج جدران النار، خصوصا تلك المبنية على ويندوز NT

*__خصائص جدران النار:__ جدران النار هي نوع خاص من البرامج الرقابية ومن خصائصها:

- أن جدران مستيقظ دائما .
- مؤمن هو نفسه ضد الاختراق.
- صغير وبسيط يسمح بالفحص الدقيق.

* __فوائد جدران النار__: من بين فوائد جدران النار أنها :

- يستعمل للتحكم بالوصول إلى الأنظمة الحساسة.
- تحمي خدمات الانترنيت غير الحصينة.
- إدارة مركزية للأمن[1]

* __تشكيل جدران النار:__ نجد نوعين من جدران النار:

- جدران النار البسيطة: وتقوم بمنع عمليات الوصول من الانترنيت لكل شئ ما عدا البريد الالكتروني الوارد.
- جدران النار مزدوج الموطن: وهي تشكيلة شائعة يجري استعمالها في الشركات التي تمتلك ملفات ويب، ويضمن وصلتين أحدهما إلى الانترنيت والأخرى إلى الشبكة الداخلية "الانترنيت"، وحركة السير هذه يمكنها أن تخرج إلى الانترنيت أو إلى طرف ثالث هو المضيف المحصن أو الملقم الذي يحتوي جدران النار [2]

3-3-3-ملقمات الانترنت:

بسبب المخاطر الأمنية المحتملة من ارتباط،الشبكة أو الأشخاص بشبكة الانترنت،فإن هذه العناصر الأخيرة تسعى لتخصص جهاز خاص يسمى proxy

[1]- داود، حسن الطاهر،المرجع السابق، ص. 368

[2]- ذياب، البداينية *الأمن وحروب المعلومات*. عمان:.دار الشروق للنشر و التوزيع.2006-ص 387

server؛ الذي يؤدي دور البوابة الخارجية Getaway لهذه الشبكات إلى شبكة الانترنت ويقوم هذا الجهاز بتصفية طلبات المغادرة عبر البوابة ،وهذه التصفية تكون على أساس تقييد عمليات وصول المستفيدين إلى مواقع معينة من الانترنت والحيلولة دون الوصول إليها أو منع الوصول في أوقات معينة أو السماح للبعض ومنع الآخرين، وبالتالي يكون الأمر مثل زجاج أحادي الاتجاه، حيث يمكن للمستخدمين الرؤية إلى الخارج لكن الدخلاء لا يمكنهم الرؤية إلى الداخل.[1] وفي حالة استخدام خدمة في خدمات الانترنت فإن الحاسوب يطلب الخدمة من الملقم الوسيط ،عندها يقوم هذا الملقم بتوجيه الطلبات إلى الملقمات الفعلية على الانترنت بالنيابة عن حواسيب الشبكة وكذا استجابة الملقمات المستهدفة لهذه الطلبات،ويقوم الملقم الوسيط بدوره بتحويل الردود إلى الحاسوب المناسب داخل الشبكة وقد تستخدم الملقمات لمنع دخول البيانات الوافدة من الانترنت إلى الكمبيوترات حيث تمنع الوصول إلى الخدمات المتوفرة على الانترنت ،والتي لا يراد أن يتمكن المستخدمين من الوصول إليها،كما يقوم لحماية الشبكات غير الحصينة.[2]

3-3-4- التشفير (Encryptions) :

مفهومه: تعتبر كلمة "تشفير" عن عملية "تحويل" أو"بعثرة" البيانات إلى هيئة غير قابلة للفهم ،وذلك بإرسالها عبر وسيلة لا يمكن لأي جهة غير جهة المقصودة تفسير هذه البيانات المبهمة، واستخلاص البيانات المفهومة منها،[3] وهي كذلك عملية تشفير المعلومات أو تحويل النص الواضح إلى نص غير مفهوم بإستعمال طريقة محددة وعمليات متسلسلة تسمى –خوارزميات التشفير- وبالتالي فإن المقصود العام من التشفير ،هو الحفاظ على سرية المعلومات بإستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز ،بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك فإنهم لا يستطيعون فهم شيء وبالتالي تحقيق سلامة البيانات.[4]

*** أنواع عملية التشفير:** وتنقسم تكنولوجيا التشفير إلى نوعين وهما:

1- المتناظر symétrique: وتستخدم فيه شفرة واحدة لكل من عملية التشفير وفك التشفير ،فيتم التشفير في الرسالة والمعلومات بإستخدام الرقم العام وكذلك في

---

[1]- سليمان داود،سرحان. ***أمن الحاسب و المعلومات***. عمان:دار وائل للنشر. 2001 .ص. 166
[2]- بات كولمان.***ترجمة مركز التعريب والترجمة: ألفا باء الانترنت***.بيروت:الدار العربية للعلوم،1998 .ص. 129
[3]- تشفير البيانات في الانترنت [متاح على الرابط] www.Dinet.co.ae/arabic/cnten net/tech0116hitm تمت الزيارة بتاريخ:2011/02/11
[4]- داود،حسن الطاهر. المرجع السابق .ص 175

نفس الوقت يتم فك الشفرة وترجمة المعلومات إلى وضعها الأصلي بإستخدام نفس الرقم العام وبالتالي استخدام مفتاح واحد للتشفير وفكه

2-**غير المتناظر Asymétrique :** ويستخدم فيه شفرة لعملية التشفير ومفتاح لفك الشفرة بمعني أن المعلومات يتم تشفيرها بالرقم العام،غير أنه لا يمكن فك الشفرة والوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام.[1]

* **مراحل وعناصر عملية التشفير**: تتألف عملية التشفير من ثلاث عناصر و هي:

1- المعلومات: التي ستجرى عليها عملية التشفير، وقد تكون رسالة نصية أو ملفات مهمة

2- خوارزمية التشفير: التي ستطبق على، المعلومات لتحويلها إلى بيانات مهمة وخوارزمية فك التشفير

3- المفتاح: هو سلسلة أو أكثر من الرموز تطبق على البيانات بإستعمال الخوارزميات التابعة.

***تقنيات التشفير:** كل يوم تظهر تقنيات جديدة مستخدمة في عملية التشفير ومن أهمها:

- تقنية مقاييس تشفير البيانات وطور من قبل شركة IBM ويعتمد طريقة المفتاح السري.

- نظام مقاييس تشفير المتطورة ويتبع تقنية تشفير جديدة وتعتمد على تقنية تشفير الكتل هي نوع متطور في طرق المفتاح السري.

- تقنية الخصوصية الجيدة: وهي تعتمد على طريقة المفتاح العام ،وهي أكثر انتشارا في مجال تشفير رسائل البريد الالكتروني ونقل وتخزن الملفات.

وعلى الرغم من هذه الأهمية القصوى والتي تبقي تحتاج إلى الكثير من أجل فهمها وإثراء موضوعها كونه موضوع واسع ويحتاج إلى الكثير من التعميق للسيطرة عليه.[2]

3-4 – برتوكولات أمن المعلومات:

يمكن تأمين نقل المعلومات اعتمادا على أسلوبين وهما :

[1]- طه. عبد الحق،المرجع السابق،ص. 257

[2]- التشفير [متاح على الرابط] URL: www.safola.com/encyption. تمت الزيارة بتاريخ:2011/02/12

❖ **الأسلوب الأول :** برتوكول نقل الأمن: تطور في سنة 1994 على يد كل من Rescoda iriquue و Alen sepmong ويعمل هذا البرتوكول من خلال طبقة التطبيق، ليعطي آلية إتصال أمنة بين الخادم و المستخدمين ،وبالتالي يعطي فرصة لعمل العديد من العمليات الآمنة من خلال العديد من التطبيقات التي تستخدمه.

❖ **الأسلوب الثاني:** برتوكول طبقة حماية الاتصال (ssc) : والذي طور من طرف شركة –نتسكيب- عام 1996 وقد لقي انتشارا سريعا كأحد أفضل بروتوكولات تأمين الإتصال عن طريق الانترنت K و أصبح مستخدما كوسيلة للتأمين في أغلب خدمات الانترنت ،وبرامج عرض الانترنت، ويسمح هذا البرتوكول لتطبيقات الخادم والمستخدم والتي تعتمد على برتوكول (IP/TCP) بالاتصال الأمن عن طريق استخدام طرق مختلفة للتشفير.

وكلا من البرتوكولين يستخدمان التوقيع الرقمي والتعريف الرقمي وطريقة التشفير عن طريق المفتاح السري، غير أن برتوكول طبقة حماية الاتصال بطبيعة عامة وغير محددة، جعلت منه الاختيار الأفضل لمصممي التطبيقات التي تستخدم برتوكول (IP/TCP) كطريقة الاتصال.[1]

3-5- خطوات أمن المعلومات:

وفيما يلي أهم خطوات الحماية الالكترونية والتي تمنح وتعطي قدرا كبيرا من الحماية للمعلومات الالكترونية:

✓ شراء نسخة أصلية وحديثة من نظام التشغيل كونه هو أساس الحماية ،كما يمكن أن يكون نقطة ضعف في الجهاز.

✓ القيام بتنزيل أحدث نسخة وإصدار من المتصفح، كون الإصدارات القديمة تحتوي على العديد من الثغرات الأمنية، وبالتالي تنزيل النسخة المدعومة بقوة التشفير 128 بت،وتعديل مستوى الأمان فيه بتعطيل التشغيل المباشر للأكتيف إكس و الجافا سكرييت.[2]

✓ إنزال نسخة أصلية وحديثة من برنامج مضاد للفيروسات، والحرص على تحديثها كل أسبوع أو كل عشرة أيام وذلك لظهور فيروسات جديدة أو معدلة كل يوم.

---

[1]- أنظمة الحماية على الانترنت،[متاح على الخط] www.Dinet.co.ae/arabic/cnten .net/tech0116hitmتمت الزيارة بتاريخ:2011/02/13

[2]- أمن المعومات ،[متاح على الخط]على الرابط www.safola.com/security.chtml/#upتمت الزيارة بتاريخ:2011/02/13

- ✓ تجنب تنزيل أي برامج مجانية، إذا لم تكن من مواقع معروفة وذات سمعة وتجنب تنزيلها من مصادر الأخبار الجماعية أو ما يعرف بـ News gnoup.
- ✓ تجنب تنزيل وفتح أو تحميل أي برنامج أو ملفات ذات طبيعة تنفذيه خاصة إن كانت من مصادر غير موثوقة .
- ✓ تجنب فتح الملفات المرفقة في الرسائل الالكترونية من مصادر غير معروفة خاصة إن كانت من نوع exe.bat cim and.
- ✓ القيام باستخدام أي برنامج لتشفير المعلومات والرسائل الالكترونية خاصة إذا كانت هذه الأخيرة في غاية الأهمية.
- ✓ تجنب الموافقة على حفظ اسم المستخدم وكلمات العبور في أي وقت وفي حالة الموافقة فسوف يتم تسهيل العملية على الهاركز و المخترقين لأنها مخزنة وجاهزة[1]

3-6- دور الجامعات والمعاهد العلمية في تطوير آلية التعامل مع النظم المعلوماتية:

مما لا شك أن المؤسسات التعليمية لها دور أساسي لأنها هي التي تعد الكوادر الأساس في مجال تقنية المعلومات ،كما أنها هي التي تقوم بالتوعية العلمية عموماً لقطاعات كبيرة من أبناء المجتمع من خلال طلاب الجامعات والمؤسسات العلمية ، وبالتالي فإن الكثير من جامعاتنا تحرص أن يكون هناك دراسات تتعلق ضمن مناهجها، ودور الجامعات أيضاً عملية على الناحية التعليمية هناك إذن جانب الأبحاث جانب التطوير في المجال ، لذلك كثير من الجهات العلمية تحرص على أن يكون هناك مؤتمرات علمية في التخصص ، ولا يخفي على أحد أن الجانب البحثي مهم أيضاً لأن الكثير من المشاكل قد تتطلب نوع من الابتكار ونوع من الاختراع لحل هذه المشاكل الأمنية المعلوماتية ، فبالتالي البحث العلمي في هذا المجال يخدم أيضاً قطاع كبير مستقبلي في التطوير.[2]

---

[1]- أمن المعومات. المرجع نفسه.

[2]- أحمد نوفل، هالة كمال. ***البيئة المعلوماتية الآمنة: المفاهيم و التشريعات و التطبيقات***. المؤتمر السادس لجمعية المكتبات و المعلومات،الرياض:(أفريل،2010)،ص.82.

خلاصة:

استحدثت نظم جديدة لتطوير حماية البرمجيات أمنياً من السرقات غير القانوني ، وذلك باعتبار أن البرمجيات هي جزء من الحواسيب وسيكون الأمن ناقصاً إذا ما أهملت أنظمة التشغيل وبقية البرامج.ولضرورة اكتمال الإجراءات الأمنية لابد أن يتم إعطاء أهمية للمواقع و المباني التي تحتوي على منظومات الحواسيب، ووفقاً لطبيعتها يتم اتخاذ إجراءات احترازية لحماية الموقع وتحصينه من أي تخريب أو سطو.



الفصل الرابع:

إجراءات الدراسة الميدانية

تمهيد :

قبل الشروع في تحليل البيانات الميدانية وتفسيرها، نود التذكير ببعض الإجراءات المنهجية التي اعتمدناها في الدراسة الميدانية؛ حيث استخدم " المنهج الوصفي" في معالجة موضوع التهديدات الأمنية للمواقع الالكترونية للجامعة الجزائرية، وكان موقع ويب جامعة منتوري قسنطينة ، هو المجال الجغرافي للدراسة، للإجابة على مجموع التساؤلات التي تضمنتها الإشكالية، و ما تفرع عنها من فرضيات. وقد تمت صياغة الفرضيات على النحو التالي:

1- سبل الحماية و الوقاية المتوفرة داخل المواقع الالكترونية كفيلة للحد من التهديدات الأمنية والتصدي لها.

2- تتفاوت انعكاسات التهديدات الأمنية على محتويات المواقع الالكترونية بحسب طبيعة تلك المحتويات.

3- ضعف أنظمة الحماية داخل المواقع الالكتروني ة يجعلها أكثر عرضة للتهديدات الأمنية.

وقد تشكلت عينة الدراسة من السيد المشرف على موقع جامعة منتوري لأنه هو الشخص الأنسب و الوحيد القادر على الإجابة على أسئلة المقابلة.

عند تفريغ المقابلة، تم ترتيب الأسئلة ترتيبا متتابعا. وقد عمدنا إلى هذا الأسلوب في تبويب أسئلة المقابلة، وترتيبها، ضمانا لوحدة الدراسة، وتوخيا للدقة في التحليل وسهولة الاستشهاد، وإمكانية الإحالة من سؤال لآخر.

4-1- تحليل البيانات وتفسيرها

المحور الأول: أنظمة الحماية المتوفرة في المواقع الالكترونية

سؤال01: ما هي أنظمة الحماية التي أثبتت نجاعتها في حماية موقعكم من التهديدات الأمنية؟

الإجابة: لا يمكنني تحديد نظام الحماية المستعمل في الموقع بالتدقيق لأنه يشكل خطرا على أمن الموقع، لكن يمكن تحديد الأنظمة بشكل عام وهي: جدران النار، Kaspersky وانترنت security.

كان الهدف من طرح هذا السؤال محاولة معرفة أنواع أنظمة الحماية المتبناة، والتي يعتمد عليها المشرف على موقع جامعة منتوري، حيث يؤكد على أنها أثبتت فعاليتها في حماية الموقع من الهجمات والاختراقات سواءاً كانت قرصنة أو فيروسات.إذ أن الملاحظ من إجابة المشرف تعطينا ثلاث أنواع من أنظمة الحماية المعتمدة: جدران النار، Kaspersky وانترنت security.

إن أنظمة الحماية الفعالة هي الركيزة الأساسية لحماية البرامج والرصيد الالكتروني بشكل عام لذا فإن اختيار نظام الحماية الجيد هو الضمان الأساسي لحماية المواقع من التلف والاختراق، كما نلاحظ أن نظام الحماية في الموقع جيد نسبيا وهذا من خلال عدم تعرض الموقع إلى اختراقات واضحة أضرت بمحتوياته إلى حد اليوم، وقد يعود هذا إلى عدم توفر الموقع على معلومات سرية أو بالغة الأهمية، هناك بعض أنظمة الحماية الأكثر شيوعا والأحسن من ناحية الجودة مثل التوقيع الالكتروني والتشفير،...، حيث أن المشرف قدم لنا أنظمة تبدو في مجملها قديمة.

سؤال 02: في رأيكم هل ضعف أنظمة الحماية كفيل بإغراء المخترقين لقرصنة موقعكم الالكتروني؟

الإجابة: بالطبع أن ضعف أنظمة الحماية المستعملة من طرف الموقع الالكتروني تغري وتجلب المخترقين.

تعد القرصنة أحد اكبر الأخطار التي تواجه المشرف على موقع جامعة منتوري نظرا للضرر الكبير الذي تلحقه بالمحتويات، إضافة إلى تكبيد الجامعة خسائر كبيرة من جراء ضياع حقوق الملكية الفكرية للأساتذة الناشرين في الموقع.

إن ضعف أنظمة الحماية هو السبب الرئيسي في تطاول المخترقين ورغبتهم في القرصنة بغرض القيام بمختلف الجرائم المعلوماتية.

سؤال 03: هل في رأيكم أن المخترقين يضعون في الحسبان درجة متانة أنظمة الحماية في موقعكم وتعددها؟

الإجابة: أول قاعدة يضعها المجرم المعلوماتي للموقع هي درجة وحصانة وقوة أنظمة الحماية المستعملة، فبالطبع في موقعنا هذا هناك حصانة ومتانة في أنظمة الحماية.

تعد درجة حصانة وقوة نظام الحماية هي القاعدة أو النظرية الأولى التي ينظر إليها المخترق، لأنها تعتبر العنصر الأساسي الذي يحدد مدى نجاح عملية القرصنة أو فشلها، أما فيما يخص موقع جامعة منتوري حسب إجابة المشرف فإنها تعتمد على نظم فعالة إلى حد كبير والدليل على ذلك ان موقعها يحتل المراتب الأولى من حيث البرامج المستعملة وأنظمة الحماية المطبقة به:

- المرتبة الأولى في الجزائر.
- المرتبة الأولى في المغرب العربي.
- المرتبة الأولى في دول إفريقيا الفرنكوفونية.

سؤال 4: ما هي المدة الزمنية المحددة لتحديث وتحيين نظم الحماية الخاصة بالموقع؟

الإجابة: قي موقعنا الالكتروني يكون تحديث نظم الحماية كل يوم لتفادي أي تهديد أو اختراق من طرف مجرمي الانترنت.

إن الهدف من طرح هذا السؤال هو محاولة معرفة المدة الزمنية التي يستغرقها المشرف لتحديث أنظمة الحماية المعتمدة في الموقع.

إن الملاحظ من إجابة المشرف أن المدة هي يوم (24 ساعة) بين العملية و العملية لكننا نقول أنها مدة طويلة مقارنة مع ما تعتمده بعض المواقع الجامعات العالمية التي وصلت إلى دقائق بين العملية و الأخرى،لذا كان لابد على المشرف بأن يعمل على تقليص مدة التحديث أكثر لتوفير حماية أكبر.

سؤال 05: هل ترون أن هذه المدة لا تعطي الفرصة لمجرمي الانترنت لقرصنة الموقع؟

الإجابة: نعم إلى حد معين، لكن لا يوجد أي تهاون من طرف المكلف على هذه العملية.

إن المدة يوم كامل هي مدة كبيرة في ظل تطور أنظمة الاختراق و القرصنة ، يقول المشرف على الموقع الالكتروني لجامعة منتوري بأنها لا تعطي الفرصة لقرصنته ،لكن هذا الشيء غير صحيح، حيث أنه إذا كانت مد ة 24 ساعة غير كافية لاختراق الموقع فلماذا تعمل بعض المواقع الأخرى على تقليص هذه الفترة إلى حد ثواني فقط ، لهذا نقول بأنها كافية لاختراق الموقع عشرة مرات أو أكثر في اليوم.

سؤال 06: ما هو مصدر نظم الحماية التي تعتمدون عليها؟

الإجابة: إن البرمجيات التي نعتمد عليها في حماية موقعنا هي مستوردة لكنها أصلية.

يعتمد الموقع الالكتروني لجامعة منتوري على أنظمة حماية مستوردة حسب إجابة المشرف وهي أصلية الصنع أي أنها مستوردة بعقود ملكية و تراخيص للاستعمال.أن استيراد أنظمة الحماية في المجال الالكتروني يعد شيء معقد ذلك أنه يحتاج إلى خبراء في الميدان لتقييم مدى فعالية النظام، إضافة إلى أنه يتطلب موارد مالية باهظة مع أنها تبقى ذات فعالية و نجاعة.

سؤال 07: إذا كانت مستوردة فما الذي يمنع من محاولة تصنيعها؟

الإجابة: ضعف ونقص في الكوادر البشرية أو بمعنى آخر نعاني من التخلف.

إن الهدف من طرح هذا السؤال هو محاولة معرفة سبب عدم اعتماد المسؤولين على الموقع الالكتروني لجامعة منتوري على أنظمة حماية محلية الصنع،لكن الملاحظ من إجابة المشرف على الموقع أن البرمجيات المحلية الصنع غير موجودة أصلا، وهذا راجع حسبه إلى ضعف تكوين الموارد البشرية الجزائرية المختصة في مجال البرمجيات و الملاحظ أنه لا توجد أية نية أو مبادرات من هذا النوع.

إن عدم محاولة القيام بمثل هذه المبادرات و محاولة تصنيع مثل هذه البرمجيات يجعل المواقع أكثر تبعية ويكلفه موارد مالية باهظة، ربما لو عملنا أو حاولنا تصنيعها محليا لوصلنا إلى نتيجة و لو مبدئية قد تجنبنا تبعات استيراد هذه البرمجيات.

سؤال08: هل هناك تعاون بينكم وبين قسم الإعلام الآلي لتصنيع بعض البرمجيات في مجال امن المعلومات؟

الإجابة: لا يوجد أي تعاون بيننا وبين قسم الإعلام الآلي ولكنه يكمن في المحتوى العلمي فقط.

تعتبر معاهد وأقسام الإعلام الآلي اكبر معاهد جامعة منتوري اهتماما بهذا المجال وذلك نظرا لطبيعة مناهجها التعليمية التي تهدف إلى تصنيع البرمجيات لذا فهي الأرضية الخصبة للاستثمار في هذا المجال(برمجيات الحماية) لكن الملاحظ من إجابة المشرف انه ليس هناك أي تعاون بين القائمين على الموقع وتلك المعاهد على الأقل لحد ألان، ففي نظره لا يمكن لهؤلاء تصنيع مثل تلك البرمجيات والتي يراها بعيدة المنال على مسؤولي تلك المعاهد، كما يقول بان التعامل مع تلك المعاهد لا يتعدى نشر رصيدهم العلمي في شكله الالكتروني على الموقع مثلهم مثل نظرائهم من باقي الأقسام.

سؤال 09: ما هي مشاريعكم المستقبلية لتطوير وتحديث نظم الحماية؟

الإجابة: لا توجد أي مشاريع وإذا حاولنا مثلا أن نصنع بعض البرمجيات في ظل تسارع وتطور نظم الحماية في عصر التكنولوجيا، يكون قد تم صنعها أكثر تطورا وحماية في البلدان المتقدمة.

لقد كان الهدف من هذا السؤال هو محاولة معرفة المشاريع المستقبلية للقائمين على الموقع الالكتروني لجامعة منتوري وتطوير وتحديث أنظمة الحماية، لكن الملاحظ من إجابة المشرف انه لا توجد أي نية للعمل على مثل هذه المشاريع، ذلك لأنه يقول إن التسارع التكنولوجي يقضي على كل مبادرة من هذا القبيل لان تصنيع مثل تلك البرمجيات يحتاج إلى سياسات رشيدة، وهذه السياسات بالنسبة للمؤسسات

المنتجة لهذه البرمجيات يجعلها أكثر تطورا إضافة إلى وجود بعض التهديدات التي تتطور بصورة رهيبة وفي حاجة إلى نظم حماية من الطراز العالي.

المحور الثاني: التهديدات الأمنية على المحتوى العلمي في المواقع

سؤال 10: ما مدى تأثير التهديدات المنية على موقعكم مقارنة بالمواقع الأخرى؟

الإجابة: تعتبر المواقع الأخرى مثل الاقتصادية والعسكرية أكثر عرضة للاختراقات من المواقع الجامعية، نظرا لأهميتها من حيث الجانب المادي بالنسبة للأولى وحيث الجانب الأمني بالنسبة للثانية.

كان الغرض من سؤالنا هذا هو معرفة أو المقارنة بين المواقع الالكترونية الجامعية بالمواقع الأخرى من تأثير التهديدات عليها وأيهما أكثر عرضة للاختراق والقرصنة، فقد تبين من إجابة المشرف أن مواقع المؤسسات الاقتصادية(التي لها نشاطات اقتصادية آو إيداعات مالية أو تحويلات من البنوك) هي الأكثر عرضة للأخطار أو لتلك التهديدات نظرا لطبيعة نشاطها المتعلق أساسا بالمعاملات المالية وعكس مواقع الجامعات مثل"موقع جامعة منتوري" التي لا تحمل في رصيدها الالكتروني تلك المعاملات المالية أو تلك الأهمية التي تغري القراصنة لاستهدافها. لهذا نستنتج أن المواقع الجامعية اقل عرضة للتهديدات الأمنية والأخطار.

سؤال 11: هل في رأيكم أن محتوى الموقع هو سبب للقيام بالتهديدات الأمنية؟

الإجابة: لقد سبق واشرنا إلى هذه النقطة حيث قلنا أن المحتوى التعليمي لا علاقة له بالتهديدات لأنه-أي المحتوى- متاح على الخط لكافة الطلبة و الأشخاص، لهذا فالمخترقون ليسو مضطرين للتخريب أو القرصنة.

من خلال هذه الإجابة فيما يخص المحتوى التعليمي والأخطار الأمنية، فان المشرف يعتبر ان المحتوى التعليمي متاح لكافة الطلبة، ولهذا يتبين لنا انه ليس هناك أي علاقة للمخترقين للمحتوى العلمي أي أن هذا الخير ليس سببا رئيسيا لاستغلاله من طرف القراصنة لتنفيذ هذه التهديدات والاختراقات

سؤال12: ما هي أسباب ودوافع المخترقين لقرصنة موقعكم بشكل عام؟

الإجابة: إن دوافع المخترقين لقرصنة واختراق موقعنا ما هو إلا عبارة عن تسلية وتباهي خاصة من بعض طلبة الإعلام الآلي.

كانت الغاية من هذا السؤال هو محاولة معرفة الأسباب الحقيقية ودوافع المخترقين لاختراق الموقع الالكتروني لجامعة منتوري ونواياهم، لكن الملاحظ من إجابة المشرف أن الأسباب والدوافع من هذه الاختراقات لا تتعدى كونها عمليات للتباهي والتسلية فقط وغالبا ما تأتي من طرف الطلبة المتمرسين الذين يجيدون لغة البرمجة ويستعملونها جيدا.

لكن عندما ننظر إلى الأمر من زاوية أخرى نقول أن القرصنة التي نتحدث عنها تتعدى بكثير كونها تسلية وتباهي وذلك لان القرصنة عملية خطيرة تهدد تلك المواقع وبالأخص أرصدتها المعرفية وبرامجها لان في حالة قرصنتها يعني ضياع حقوق الملكية الفكرية وهي في الغالب للأساتذة والباحثين والناشرين داخل الجامعة، إضافة إلى استنساخ هويات الطلبة والأساتذة وهي تأتي في الغالب من طرف مخترقون يعرفون محيط الجامعة جيدا ويعملون على تزوير وسرقة تلك المعلومات الهامة.

سؤال13: ما هو المحتوى التعليمي الأكثر عرضة وتضررا من هذه الاختراقات؟

الإجابة: لا توجد أي تهديدات على المحتوى التعليمي لأنها متاحة على الخط.

كان الغرض من طرح هذا السؤال هو معرفة المحتوى الأكثر عرضة للقرصنة في الموقع الالكتروني لجامعة منتوري جراء هاته التهديدات. حيث كانت إجابة المشرف أن المحتوى العلمي المتاح على الخط غير معرض لهذه الاختراقات ومن هنا تبين لنا انه ليس هناك سبب حقيقي لقرصنة الموقع وإنما الأسباب الحقيقية لها أغراض أخرى ذكرناها سابقا.

سؤال 14: هل نظم الحماية المعتمدة كفيلة بحماية المحتوى التعليمي لموقعكم؟

الإجابة: قلنا أن المحتوى التعليمي متاح على الخط إي انه لا توجد أخطار تهدد هذا ألمحتوى.

لقد حاولنا خلال طرح هذا السؤال معرفة قدرة نظم الحماية على تامين المحتوى التعليمي المتاح على الموقع، فكانت إجابة المشرف على الموقع مشابهة تماما للجواب السابق أي انه لا توجد مخاطر على المحتويات العلمية، وفيما يخص أنظمة الحماية تطرق إلى أنها تحمي الموقع ككل وليس جزء خاص منه.

سؤال15: ما مدى قناعة الأساتذة الناشرين داخل الموقع بهذه النظم.

الإجابة: لا يوجد أي دخل للأساتذة الناشرين في هذا الموضوع.

وحول ثقة الأساتذة الناشرين في نظم الحماية المعتمدة من طرف إدارة الموقع ارتأينا طرح هذا السؤال على المشرف ليجيبنا انه لا دخل للأساتذة في شؤون إدارة الموقع، وكذلك لأنهم يعلمون إن منشوراتهم متاحة لجميع مستعملي الموقع وهنا تبين لنا أنهم "الأساتذة" لا يهتمون بهذه الأشياء.

سؤال16: ماهية الطرق التي يتم فيها حماية المحتوى؟

- عند الإيداع.

- عند الاسترجاع.
- عند الحفظ.

الإجابة: الطرق التي يتم فيها حماية المحتوى هي عند الإيداع.

تعتبر مصادر الخطر على امن المحتوى كثيرة جدا، ولعل من أهمها الوصول إلى البيانات من قبل أشخاص غير مسموح لهم وبالتالي يتم تسرب المعلومات وإتلافها أو تغييرها فالطريقة التي يتبعها مسؤول الموقع عند حماية المحتوى هي أثناء عملية الإيداع لتفادي إي خطر على أمنها باعتبارها أحسن طريقة عند المشرف.

سؤال17: ما هي أشكال الملفات التي تعتمدونها والتي تكفل المحتوى التعليمي؟

الإجابة: هناك شكل واحد وهو PDF.

تم طرح هذا السؤال لمعرفة أهم الأشكال التي يتبعونها لحفظ المحتوى التعليمي في الموقع، فهناك العديد من أشكال الملفات منها , PDF,HTM , XML لكن الموقع يعتمد على شكل الملف PDF لأنه الشكل الأفضل حسب إجابة المشرف والأمن لحماية الملفات من عمليات النسخ والتزوير وغيرها من عمليات السرقة والقرصنة.

سؤال18: هل تتعرض المعلومات أثناء مسارها في رحلة البث والاسترجاع إلى إخطار أمنية؟

الإجابة: لا تتعرض معلوماتنا المنشورة في الموقع إلى تهديدات أمنية .

أما بخصوص تعرض المعلومات أثناء مسارها في رحلة البث والاسترجاع يجب ان تخضع لرقابة دقيقة من حيث الوصول إليها إلا من هو مصرح له من خلال البوابات الآمنة التي تعتمد على التقنيات المتقدمة من خلال التشفير والملاحظ من إجابة المشرف أنها لا تتعرض إلى أية أخطار إنما توجد مخاطر على الموقع بشكل عام.

سؤال19: ما طبيعة هذه التهديدات؟

بدون إجابة.

المحور الثالث: مقاومة أنظمة الحماية للتهديدات على المواقع

سؤال20: ما هي طرق الحماية المعتمدة في موقعكم بشكل عام؟

الإجابة: هناك محور يدعى info programme فهو متاح على الخط لكن هناك محور يسمى prive programme وهو محاط بأنظمة الحماية المذكورة سابقا ويكون التجديد والتحديث كل يوم في هذه الأنظمة لتفادي الأخطار الأمنية.

طرح هذا السؤال لمعرفة أهم الطرق المستعملة في امن وحماية الموقع من التهديدات المنية الخارجية، والملاحظ من إجابة المشرف أن هناك عدة طرق لحماية الموقع وتتبعه عدة بروتوكولات الحماية، ويلخصها المشرف في محورين: info programme المتاحة على الخط وهناك المحور الأخر هو prive programme وهذا الأخير الذي يتمتع بأنظمة الحماية العالية الجودة مثل internet sécurité وعدة أنظمة أخرى ولكن حسب المشرف دائما انه يتعين عليه تجديد و تحديث لهذه الأنظمة لتفادي تقادمها وكذلك عدم السماح للمخترق من اكتشاف الثغرات الأمنية فيها.

السؤال21: هل يمكن اعتبار التكنولوجيا الحديثة في مجال الحماية أداة نوعية كافية لحماية موقعكم؟

الإجابة: كافية لكن هناك مشكلة في المتخصصين في المجال لتكملة ما جاءت به هذه التكنولوجيا.

لقد أدت التكنولوجيا الحديثة ثورة في مجال الإعلام الآلي، فكما أن للتكنولوجيا ايجابياتها لها سلبياتها ومن بين ايجابياتها: أن هناك عدة طرق وأنواع للحماية الفعلية للمواقع، ولكن حسب المشرف انه لا تستغل التكنولوجيا أحسن استغلال كذلك عدم وجود مختصين أكفاء يتابعون ويطورون هذه الميزة، كما استغلها بعض الهاكرز والكراكرز لتحقيق أهدافهم فهي تساعدهم على الاختراق بأشكال متعددة.

السؤال22: هل هناك أسباب لارتكاب الجريمة الالكترونية على موقعكم؟

الإجابة: قلنا سابقا أنها للتباهي فقط.

وحول الأسباب الحقيقية التي تجعل المخترقين يحجبون ويهددون امن الموقع فقد قال المشرف انه لا توجد أسباب حقيقية وراء هذه الإعمال وإنما السبب حسبه هو التباهي والتسلية مما يؤدي إلى ارتكاب الجرائم الالكترونية.

السؤال23: ما هي اثار التهديدات التي يخلفها كالها كرز والكراكرز على الموقع؟

الإجابة: إفساد برامج الموقع بشكل عام.

غالبا ما يكون لكل جريمة سبب ولكن الملاحظ أن للمخترقين دوافع وأسباب لا يعلمها سواهم، مما يخلف أضرار على الموقع حسب ما أكده المشرف على امن موقع جامعة منتوري، حيث تعرض الموقع إلى عدة اختراقات مما افسد برامجه وعمله بشكل عام قد تستمر لعدة ساعات وفي بعض الحالات إلى أيام.

السؤال24: هل يتعرض الموقع إلى جميع أنواع التهديدات؟

الإجابة: يتعرض الموقع إلى بعض التهديدات مثل: الفيروسات، مجرمو المعلومات كالهاكرز والكراكرز.

وحول أنواع التهديدات التي يتعرض لها موقع UMC أجابنا المشرف أن أهم المخاطر التي يواجهها هي: الفيروسات ومجرمو المعلومات والإنترنت، والملاحظ هنا أن اغلب التهديدات التي تهدد امن الموقع إما أن تكون فيروسات تتنقل من حاسب إلى أخر بواسطة الرسائل الالكترونية أو الملفات المرفقة أو الأجهزة القابلة للإزالة flash disque أو روابط نصية مجهولة المصدر.

السؤال25: ما هي أهم الأخطار التي تواجه امن موقعكم في ظل تسارع وتطور نظم الاختراق والقرصنة؟

الإجابة: في الوقت الحالي لا نواجه الكثير من التهديدات.

في ظل تسارع وتنامي ظاهرة الاختراق وتطور النظم التي تساعدها على ذلك طرحنا السؤال على المشرف حول ماهية الأخطار التي تواجه امن الموقع، فكانت إجابته انه لا توجد أي تهديدات تتربص بالموقع باستثناء بعض الحالات التي ذكرناها سابقا، وذلك راجع إلى نقص قيمة المحتويات في الموقع عند المخترقين وقراصنة الانترنت، والذين يريدون الاستفادة وتحقيق مكاسب من وراء عملياتهم الإجرامية.

السؤال26: ما مدى مقاومة نظم الحماية المعتمدة من طرفكم للتهديدات الأمنية؟

الإجابة: تحقق 90% من المقاومة.

إن قياس مدى مقاومة أنظمة الحماية المعتمدة من طرف القائمين على الموقع يرتبط أساسا بوعي المسؤولين على امن الموقع ونظرتهم الشاملة، حيث تحقق أنظمة الحماية المستعملة حوالي 90% من المقاومة والحماية وذلك راجع حسب رأينا إلى كيفية وحسن اختيار النظم الكفيلة بحماية الموقع والعمل على تطويرها وتحسينها وكذلك تحيينها.

من خلال هذه المقابلة التي أجريناها مع المشرف على موقع جامعة منتوري اتضح لنا، انه يولي اهتماما اكبر بحماية الموقع دون المحتوى الفكري المودع من طرف الأساتذة، اعتقادا منه أن حماية المحتوى من حماية الموقع.

4-2- النتائج العامة للدراسة:

1 - بعد إجرائنا لهذه الدراسة وإبراز أهم التهديدات وطرق الحماية ودور المواقع في دعم وتطوير العملية التعليمية والبحث العلمي من خلال استخدامها من طرف الأساتذة والطلبة بصفة عامة وعلى ضوء هذا توصلنا إلى مجموعة من النتائج:

2 - أنظمة الحماية المستعملة في الموقع الالكتروني لجامعة منتوري أثبتت نجاعتها في الحد من التهديدات الأمنية.

3 - ضعف أنظمة الحماية كفيل بإغراء المخترقين لقرصنة الموقع.

4 - طبيعة محتوى الموقع له تأثير على اختراق الموقع.

5 - المحتوى التعليمي للموقع الالكتروني متاح لكافة الطلبة والأساتذة والأشخاص على الخط.

6 - برامج الموقع الالكتروني هي الأكثر عرضة للتهديدات والاختراقات.

7 - نظم الحماية المتبعة بالموقع الالكتروني لجامعة منتوري تحقق 90% من المقاومة.

8 - استعمال الموقع الالكتروني لنظم حماية مستوردة أصلية الصنع

9 - انعدام المشاريع والأفاق المستقبلية لتطوير وتحديث نظم الحماية للموقع الالكتروني لجامعة منتوري قسنطينة.

10 - لا يوجد تعاون وتنسيق بين المسؤولين على الموقع وأقسام الإعلام الآلي لتصنيع برمجيات الحماية.

11 - نقص في متخصصي الإعلام الآلي لمواكبة التكنولوجيا وتطوير نظم الحماية.

4-3- نتائج الدراسة على ضوء الفرضيات:

الفرضية الأولى:

والتي توقعت أن سبل الحماية و الوقاية المتوفرة داخل المواقع الالكترونية كفيلة لحد من التهديدات الأمنية والاختراقات و التصدي لها.

الفرضية تحققت وذلك من خلال المقابلة التي تمت مع المشرف على حماية وأمن موقع جامعة منتوري قسنطينة و التي تمثلت مؤشراتها فيما يلي :

- إن أنظمة الحماية المستعملة في الموقع الالكتروني قد أثبتت فعاليتها ويتجسد ذلك في الأنظمة التي يعتمدونها في الحماية و هي:

* جدران النار .

* انترنت سيكيريتي.

*كاسبرسكي.

- احتلال الموقع الالكتروني لجامعة منتوري قسنطينة المرتبة الأولى في الجزائر و المغرب العربي و دول إفريقيا الفرنكوفونية في جملة الخصائص و المميزات من أبرزها نضم الحماية.

- استعمال الموقع لبرمجيات أصلية فعالة مستوردة و هذا ما يعكس سبب نقص التهديدات

وعليه فإن الفرضية قد تحققت.

الفرضية الثانية:

والتي نصت على ما يلي:

تتفاوت انعكاسات التهديدات الأمنية على محتويات المواقع الالكترونية بحسب طبيعة المواقع وقد تمثلت مؤشراتها فيما يلي:

- إذا ما نضرنا إلى إجابة المشرف على أسئلة المحور الثاني التي كانت حول تأثير التهديدات الأمنية على المحتوى مقارنة بالمواقع الأخرى فنجد:

- المحتوى العلمي للموقع الالكتروني لجامعة منتوري قسنطينة لكافة الطلبة و الباحثين و لكل مستعملي الموقع و عليه فإنه لا توجد أي تهديدات بغرض سرقة المحتوى العلمي.

- إن الموقع الالكتروني لجامعة منتوري قسنطينة لا يتصفحه أغلبية الناس فهو غالبا ما يستغل من طرف الطلبة و الباحثين ولهذا فهو غير مهم لعامة الناس أو بالأحرى للمخترقين وهذا ما يعني نقص إن لن لم نقل أي تهديدات .

- إن الموقع غير مهم مقارنة بالمواقع الالكترونية الأخرى مثل المواقع الاقتصادية و العسكرية و التي تتعرض لعديد من الهجمات و الاختراقات بغرض سرقة المحتوى و هذا ما تعبر عنه الإجابة الأولى في المحور الثاني.

و هذا لا ينفي وجود بعض محاولات الاختراق لموقع من طرف بعض طلبة الإعلام الآلي بالجامعة لغرض التباهي و التسلية فقط وليس هناك أي نية لسرقة المحتويات.

وبهذا فإن الفرضية قد تحققت.

<u>الفرضية الثالثة:</u>

والتي توقعت أن ضعف انظمه الحماية داخل المواقع الالكترونية يجعلها أكثر عرضة للتهديدات الأمنية.

وبعد الدراسة و التحليل تم التوصل بأن الفرضية محققة وتمثلت مؤشراتها فيما يلي :

- أن الموقع الالكتروني لجامعة منتوري قسنطينة أصبح لا يتلقى تهديدات بعدما تم الاعتماد على برمجيات ونضم فعالة في حمايته عكس ما كان عليه في الماضي حيث كان يعتمد على برمجيات قديمة وغير أصلية.
- إن أنظمة الحماية التي يعتمد عليها الموقع تحقق نسبة 90بالمائة من المقاومة نتيجة حسن اختيارها.

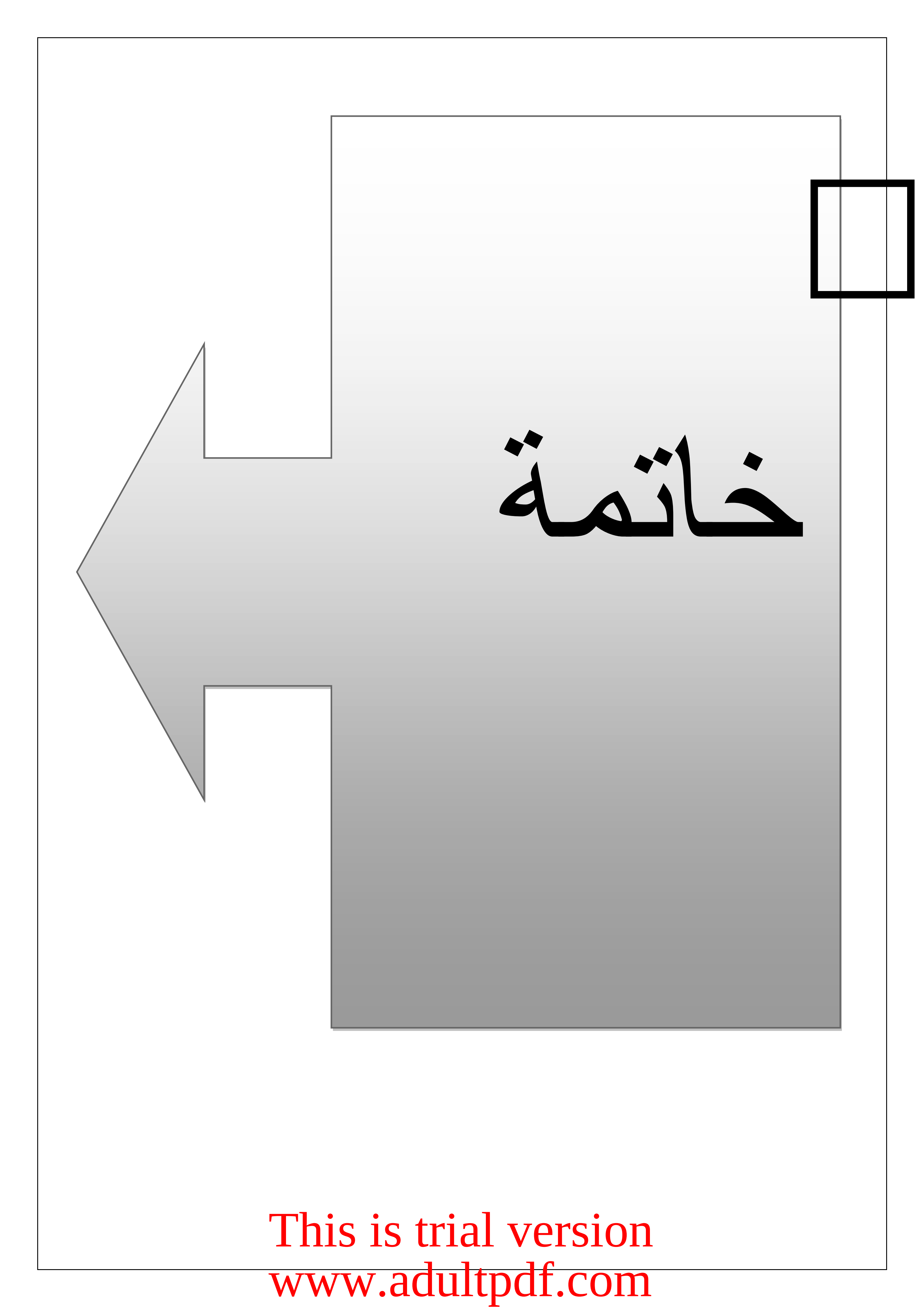
وعلى هذا فإن الفرضية تحققت.

4-4-الاقتراحات:

وعليه ومن خلال النتائج المتوصل إليها نستخلص أن البيئة الالكترونية ورغم الايجابيات الكبيرة و الآفاق التي فتحتها للعالم، إلا أنها لا تخلو من الكثير من الانتهاكات و التصرفات غير القانونية مما يؤدي إلى خلق تخوف من استعمالها و الحد من مصداقيتها، ومن هنا يبرز الدور الفعال الذي يكتسيه أمن المعلومات داخل البيئة الالكترونية حيث يعد عاملا مهماً لاستمرار انسيابية المعلومات و تداولها وإتاحتها.

و نحاول من خلال النقاط التالية تقديم بعض الاقتراحات لنكون بهذا قد خطونا خطوة نحو إرساء مجتمع معلومات آمن:

- التحسيس بضرورة أمن المعلومات من خلال عقد الندوات والمؤتمرات وطرح ما توصل إليه العلم في هذا المجال.
- تفعيل التعاون العربي و الدولي في مجال المعلوماتية وأمنها لأجل تبادل الخبرات.
- تحسين و تطوير و تحيين أنظمة الحماية لمواجهة كل الأخطار المحتملة على الموقع وأمنه.
- الاعتماد على سياسة التكوين الجيد للمشرفين على أمن وحماية المواقع من خلال القيام بدورات تدريبية مع إرسال بعثات إلى الخارج.
- ضرورة تعديل القوانين و التشريعات التي تساعد على حماية الملكية الفكرية و حقوق المؤلفين.
- ضرورة توخي الحذر من بعض الفيروسات أثناء التعامل مع أطراف خارجية في إطار تبادل المعلومات و الخبرات.
- الاهتمام أكثر بحماية المحتوى الفكري المودع من طرف الأساتذة و الباحثين من السرقات العلمية وهذا ما يؤدي إلى عزوف الأساتذة عن النشر داخل المواقع.


خاتمة

خـــــــــــاتمة :

يبرز دور المواقع الالكترونية بشكل جلي في تطوير وترقية البحث العلمي من اجل المساهمة في اللحاق بالعالمية المتقدمة, مما يحتم على الجامعات المشاركة في هذه التقنية بغية تطوير وترقية بحوثنا العلمية.

إلا أن البيئة الالكترونية ورغم الايجابيات الكبيرة والأفاق التي قدمتها للعالم، إلا أنها لا تخلو الكثير من الانتهاكات و التصرفات غير القانونية؛ مما يؤدي إلى خلق تخوف من استعمالها والحد مـــن مصداقيتها، ومن هنا يبرز الدور الفعال الذي يكتسيه امن المعلومات حيث يعد عاملا مهما لاستمرار انسيابية المعلومات وتداولها وإتاحتها.

وعلى هذا الأساس لابد من تكاثف الجهود وسن تشريعات وقوانين للحـــد مـــن هـــذه الاختراقات وردع مرتكبيها؛ لان العالم اليوم يسير بخطى متسارعة نحو تكريس قرية كونية قوامهـــا المعلومات والشبكات، وعلى هذا نأمل أن نجد لأنفسنا بيتا في هذه القرية وهذا لا يأتي إلا بالعمـــل الجاد و الطموح والإرادة الصادقة من كافة الجهات الفاعلة في المجتمع.

قائمة المختصرات:

UMC : Université Mentouri Constantine

FTP : Files Transfer Protocol.

HTML : HyperText Markup Language

HTTP : HyperText Transfer Protocol

TCP/IP: Transfer Control Protocol /Internet Protocol

URL: Uniform Resource Locator

GIF: Graphic Inter change Format


قائمة المراجع

قـــــائمة المـــــراجع

المعاجم باللغة الأجنبية:

1- Voss,Andrés. Dictionnaire de l'informatique et de l'anterret 1999 paris: micro .application 1998.

الكتب باللغة العربية:

2 - بات كولمان، **ترجمة مركز التعريب والترجمة :ألفا باء الانترنت**. بيروت:الدار العربية للعلوم،1998.

3 - الجبري، خالد بن عبد الرحمان، **تقنية مواقع المعلومات المتاحة على الانترنت**. الرياض : مجلة مكتبة الملك فهد الوطنية،نوفمبر1999.

4 - داوود،حسن الطاهر، **الحاسب وأمن المعلومات** ، الرياض:مكتبة الملك فهد الوطنية.2000 .

5 - دايسون بيتر، **ألفباء الانترنت**. لبنان: دار العربية 1988.

6 - ذياب، البداينية ، **الأمن وحروب المعلومات**. دار الشروق للنشر و التوزيع.2006.

7 - سليمان داود،سرحان ، **أمن الحاسب و المعلومات**. عمان:دار وائل للنشر،2001 .

8 - شاهين ، بهاء. **المرجع العلمي لاستخدام الانترنت**.القاهرة : دار العلوم العربية،1997.

9 - شاهين، بهاء، **شبكة الانترنت**.مصر : كبيوسينس، 1996 .

10 - شوقي،حسام ، **حماية وأمن المعلومات على الانترنت**.القاهرة:دار الكتب العلمية،2003.

11 - صادق،دلال؛الفتال، حميد ناصر، **أمن المعلومات**.عمان :دار اليازوري العلمية، 2008.

12 - الضامن ، منذر، **أساسيات البحث العلمي**.(ط.1)، عمان : دار المسيرة للنشر و التوزيع، 2009 .

13 - طه. عبد الحق، **مدخل إلى المعلوماتية: العتاد و البرمجيات**، الجزائر :قصر الكتاب. 2000.

14 - عبد الله حسين،علي محمود، **سرقة المعلومات المخزنة في الحاسب الآلي**.القاهرة:دار النهضة،2001.

15 - عليان، ريحي مصطفى؛غنيم عثمان محمد. **أساليب البحث العلمي:الأسس النظرية و التطبيق العلمي**،(ط.2)،عمان:دار صفاء للنشر و التوزيع. 2008.

16 - غربي ، علي . **أبجديات منهجية في كتابة الرسائل الجامعية**. قسنطينة : Cirta Copy ، 2008 .

17 - محمد،فاروق العامري،**الانترنت**،القاهرة:دار الفكر العربي ،1997.

18 - مود اصطفان، هاشم. **منهجية ومقاييس تقييم المواقع على الشبكة العنكبوتية: الإستراتيجية الموحدة للمعلومات في عصر الانترنت ودراستها** . 1998.

المراجع باللغة الأجنبية:

19- Bouche, gille.**tout savoir sur enternet**.paris : ARLEA, 1996.

20- Kent, péter.**le world wide web** paris: samad SM,1995.

المذكرات:

21 - بليرون ،نادية. تصميم مواقع البحث دعامة للشبكة الأكاديمية البحثية ، ليسانس:علم المكتبات: قسنطينة.2003

22 - رحابي ، توفيق؛ سلطاني،عبد المجيد. الانترنت و إتاحة المعلومات داخل المحيط العلمي :دراسة ميدانية بجامعة منتوري: ليسانس: علم المكتبات: قسنطينة،2000

23 - سيدهم ، خال د هناء.المراسلات الالكترونية داخل محيط البحث العلمي.جامعة منتوري قسنطينة:قسم علم المكتبات؛1999

24 - غانم، نذير. تقييم مواقع الويب الجزائرية على الانترنت . ماجستير: علم المكتبات :قسنطينة،2002

25 - غزال، عبد الرزاق .أمن المعلومات الالكترونية وحق المؤلف في ضل التشريع الجزائري. ليسانس :علم المكتبات :قسنطينة، جامعة منتوري، 2002.

متفرقات:

26 - أحمد نوفل، هالة كمال .البيئة المعلوماتية الآمنة: المفاهيم و التشريعات و التطبيقات. المؤتمر السادس لجمعية المكتبات و المعلومات،الرياض:(أفريل،2010).

27 - صابر،دويب حسين.المؤتمر السادس لجمعية المكتبات و المعلومات السعودية. الرياض: (افريل، 2010).

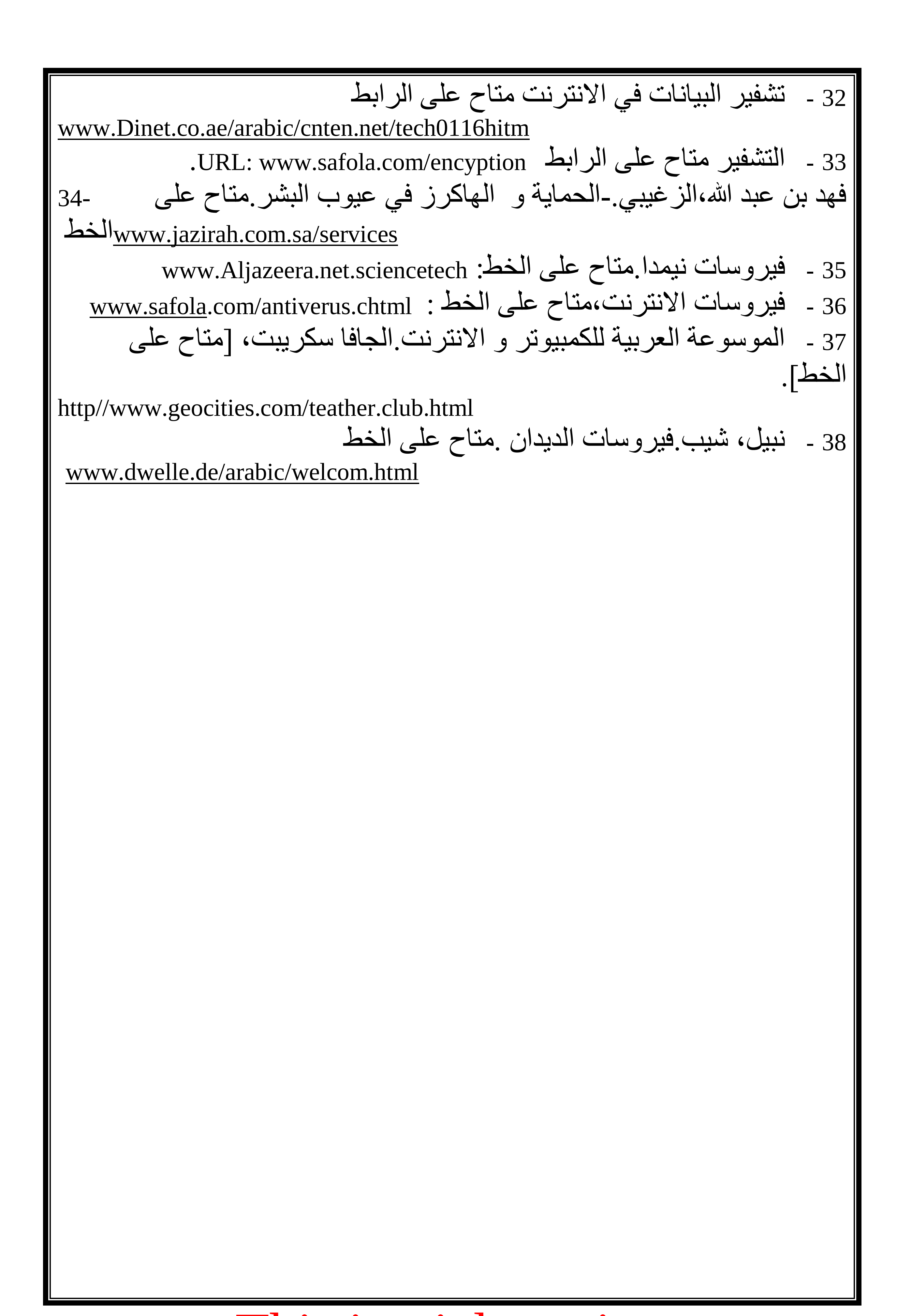
الويبو غرافيا:

28 - أمن المعلومات. متاح على خط: URL:safola.Com/security. chtml.
أنظمة الحماية على الانترنت،متاح على الرابط :
www.Dinet.co.ae/arabic/cnten.net/tech0116hitm

29 - برامج ذاتية التحميل متاح على الخط www.safola.com/exc.programe.chtm

30 - برامج ذاتية التحميل. متاح على الخط www.Safola.com/exc-programe.chtml

31 - برنامج الأشرار وأسلحة الهاكرز.متاح على الخط
www.Safola.com/lolis.chtml



32 - تشفير البيانات في الانترنت متاح على الرابط
www.Dinet.co.ae/arabic/cnten.net/tech0116hitm

33 - التشفير متاح على الرابط URL: www.safola.com/encyption.

34- فهد بن عبد الله،الزغيبي.-الحماية و الهاكرز في عيوب البشر.متاح على الخطwww.jazirah.com.sa/services

35 - فيروسات نيمدا.متاح على الخط: www.Aljazeera.net.sciencetech

36 - فيروسات الانترنت،متاح على الخط : www.safola.com/antiverus.chtml

37 - الموسوعة العربية للكمبيوتر و الانترنت.الجافا سكريبت، [متاح على الخط].
http//www.geocities.com/teather.club.html

38 - نبيل، شيب.فيروسات الديدان .متاح على الخط
www.dwelle.de/arabic/welcom.html


الملاحق:
□أسئلة المقابلة

أسئلة المقابلة:

المحور الأول: أنظمة الحماية المتوفرة في المواقع الالكترونية

السؤال 01: **ما هي أنظمة الحماية التي أثبتت نجاعتها في حماية موقعكم من التهديدات الأمنية؟**

السؤال 02: **في رأيكم هل ضعف أنظمة الحماية كفيل بإغراء المخترقين لقرصنة موقعكم الالكتروني؟**

السؤال 03: **هل في رأيكم أن المخترقين يضعون في الحسبان درجة متانة أنظمة الحماية في موقعكم وتعددها؟**

السؤال 04: **ما هي المدة الزمنية المحددة لتحديث وتحيين نظم الحماية الخاصة بالموقع؟**

السؤال 05: **هل ترون أن هذه المدة لا تعطي الفرصة لمجرمي الانترنت لقرصنة الموقع؟**

السؤال 06: **ما هو مصدر نظم الحماية التي تعتمدون عليها؟**

السؤال 07: **إذا كانت مستوردة فما الذي يمنع من محاولة تصنيعها؟**

السؤال 08: **هل هناك تعاون بينكم وبين قسم الإعلام الآلي لتصنيع بعض البرمجيات في مجال امن المعلومات؟**

السؤال 09: **ما هي مشاريعكم المستقبلية لتطوير وتحديث نظم الحماية؟**

المحور الثاني: التهديدات الأمنية على المحتوى العلمي في المواقع

السؤال 10: **ما مدى تأثير التهديدات المنية على موقعكم مقارنة بالمواقع الأخرى؟**

السؤال 11: **هل في رأيكم أن محتوى الموقع هو سبب للقيام بالتهديدات الأمنية؟**

السؤال 12: **ما هي أسباب ودوافع المخترقين لقرصنة موقعكم بشكل عام؟**

السؤال 13: **ما هو المحتوى التعليمي الأكثر عرضة وتضررا من هذه الاختراقات؟**

السؤال 14: **هل نظم الحماية المعتمدة كفيلة بحماية المحتوى التعليمي لموقعكم؟**

السؤال 15: **ما مدى قناعة الأساتذة الناشرين داخل الموقع بهذه النظم؟**

السؤال 16: **ماهية الطرق التي يتم فيها حماية المحتوى؟**

السؤال 17: **ما هي أشكال الملفات التي تعتمدونها والتي تكفل المحتوى التعليمي؟**

السؤال 18: **هل تتعرض المعلومات أثناء مسارها في رحلة البث والاسترجاع إلى إخطار أمنية ؟**

السؤال 19: **ما طبيعة هذه التهديدات؟**

المحور الثالث: مقاومة أنظمة الحماية للتهديدات على المواقع

السؤال 20: **ما هي طرق الحماية المعتمدة في موقعكم بشكل عام؟**

السؤال 21: **هل يمكن اعتبار التكنولوجيا الحديثة في مجال الحماية أداة نوعية كافية لحماية موقعكم؟**

السؤال 22: **هل هناك أسباب لارتكاب الجريمة الالكترونية على موقعكم؟**

السؤال 23: **ما هي اثار التهديدات التي يخلفها كالها كرز والكراكرز على الموقع؟**

السؤال 24: **هل يتعرض الموقع إلى جميع أنواع التهديدات؟**

السؤال 25: **ما هي أهم الأخطار التي تواجه امن موقعكم في ظل تسارع وتطور نظم الاختراق والقرصنة؟**

السؤال 26: **ما مدى مقاومة نظم الحماية المعتمدة من طرفكم للتهديدات الأمنية؟**

الملخص:

أصبحت الجرائم المعلوماتية تشكل تهديداً و تحدياً خطيرً للمواقع الالكترونية ، و افتقار الكثير من دول العالم لقوانين خاصة لمواجهة هذه الجرائم المدمرة في الفضاء الإلكتروني لتحقيق أهدافها التخريبية و اختراق نظم الحماية في المواقع.

و قد جاءت دراستنا لتتناول الموضوع وتتبعه من خلال أهم التحولات التي مست المواقع الالكترونية مع محاولة تبيان مدى تأثير التهديدات الأمنية على المواقع الالكترونية ونظم الحماية.

وعليه اتخذنا هذا الشكل الحديث لموضوع بحثنا الذي جاء بعنوان " التهديدات الأمنية في المواقع الالكترونية للجامعة الجزائرية–دراسة ميدانية بموقع جامعة منتوري–" ومن خلال هذا المجال الميداني الذي قمنا به ضمن هذا البحث لمعرفة حجم الأخطار التي تواجه أمنية المواقع الالكترونية وطرق الحماية المعتمدة ارتأينا الاعتماد فيه على منهجية تتماشى مع هذه المواضيع متمثلة في :

المنهج الوصفي الذي اعتمدناه لبناء الفصل النظري و تحليل بيانات المقابلة ، كما حاولنا وضع بعض الاقتراحات حول ضرورة حماية مواقع الويب بصفة عامة و المحتوى الفكري داخله بصفة خاصة.

الكلمات المفتاحية:

المواقع الالكترونية – الجرائم المعلوماتية – أمن المعلومات – تكنولوجيا المعلومات – الانترنت – جامعة قسنطينة.

Résumé :

Les crimes de l'information ont à devenu une menace qui défie les cites électroniques, et l'absence des lois dans plusieurs pays du monde qui lutte contre ses crimes distractifs de l'espace électronique, et qui pentues les systèmes de sécurité des cites

Et en a consacrer notre étude se sujet et suivre les important

tournant qui a touché les cites électronique et montrer sont influence de ses menace les cites électronique et les système de sécurité.

Pour cella en a prés cette nouvelle forme au notre sujet d'étude intitule « les menaces sécurité dans les cites électronique de université algérienne –étude pratique sur le cite web de université mentoré /www.umc-edu.com.

A partir de cette étude qu'on a fait pour rendre compte d volume de risque qui menace la sécurité des cites électronique, et les système de sécurité adapté pour les protégé on a unliser une méthode compatible avec se jenre d'étude qui est la méthode descriptive pour les chapitres théorique et analytique pour les données pratique, comme on a mois quelques proposition a proposé de la nécessité de sécurité des cites web en générale, et leur contenu en particules

Mots clé :

Les cites électronique – les crimes d'information –sécurité l'information –technologie de l'information –internet –université de constantine.

Abstract :

IT crimes have become a threat and a serious challenge to the websites, and the lack of much of the countries to special laws to deal with these devastating crimes in cyberspace to achieve the objectives of sabotage and penetration protection systems at the sites .

And came to our study on the subject and followed through the most important changes that touched the web sites with an attempt to demonstrate the impact of security threats to websites and protection systems .

So we took this modern form the subject of our research, which was entitled "security threats in the websites of the University of Algeria - a field study site University Mentouri -" It is through this field the field that we have done in this research is to determine the size of the risks faced by the security Web sites and protection methods adopted we decided to rely where the methodology in line with these themes represented in:

Descriptive approach, which we have to build a theoretical chapter, and the analytical method for the analysis of interview data, as we have tried to put some proposals on the need to protect Web sites in general and within the intellectual content in particular .

Keys words :

Web sites - IT crimes - Information Security - Information Technology - Internet - University of Constantine